M6sWschFredactedCorrected

1  UNITED STATES DISTRICT COURT
   SOUTHERN DISTRICT OF NEW YORK
2  ------------------------------x

3  UNITED STATES OF AMERICA,

4              v.                           17 Cr. 548 (JMF)

5  JOSHUA ADAM SCHULTE,

6              Defendant.
                                           Trial (Redacted)
7  ------------------------------x

8                                          New York, N.Y.
                                           June 28, 2022
9                                          9:05 a.m.

10  Before:

11
                        HON. JESSE M. FURMAN,
12
                                           District Judge
13                                         -and a Jury-

14                              APPEARANCES

15  DAMIAN WILLIAMS
         United States Attorney for the
16       Southern District of New York
    BY:  DAVID W. DENTON JR.
17       MICHAEL D. LOCKARD
         Assistant United States Attorneys
18

19  JOSHUA A. SCHULTE, Defendant *Pro Se*

20

    SABRINA P. SHROFF
21  DEBORAH A. COLSON
         Standby Attorneys for Defendant
22
    Also Present:  Charlotte Cooper, Paralegal Specialist
23

24

25

M6sWsch1

1              (Trial resumed; jury not present)

2              THE COURT:  Good morning.  I hope all are well.

3              A number of issues to discuss this morning.  Before I

4    get there, though, have we implemented the lockdown, limited

5    lockdown, limited closure that I have authorized, Mr.

6    Hartenstine?

7              MR. HARTENSTINE:  Yes, your Honor.

8              THE COURT:  And I take it that the overflow is working

9    and folks there should be able to hear?

10             MR. HARTENSTINE:  That's correct, your Honor.

11             THE COURT:  All right.

12             I want to triage and focus on the things that need to

13   be discussed this morning, since I'll check on the jury in a

14   moment, but I would like to get started with the witness as

15   soon as we can.

16             A few things.  First, after weighing the two bad

17   options, I've decided that we should skip next Tuesday to

18   preserve, keep that juror on the jury.  Having lost one, and

19   given risks of losing others, to Covid or otherwise, it just

20   feels to me like that is the least bad option.  In exchange,

21   and to mitigate the downside of losing a trial day, I'm going

22   to ask the jury to be prepared next Wednesday and Thursday to

23   sit slightly longer days and possibly keep them until four or

24   even 4:30.  So I'm giving you a heads-up about that, and you

25   should plan accordingly as well.  Bottom line is we will not

1    sit Friday and we will not sit Tuesday.  It's not ideal, but

2    again, it's the least bad option, as far as I'm concerned.

3            Second, I wanted to just circle back and make more of

4    a record on the Berger issue with respect to the NetFlow

5    records, because it occurred to me that while Mr. Schulte's

6    point about going beyond the scope was well-taken -- that is to

7    say, that he had identified Mr. Berger as one of the witnesses

8    that he would have called as part of his own case -- there's a

9    flip-side problem there, which is to the extent that he would

10   call him as part of his own case to elicit testimony about

11   those records, it would be expert testimony and he had to

12   notice him, and having not noticed him, that is another reason

13   that he should not have been permitted to go there yesterday.

14   So I wanted to circle back on that.

15           The other issues on my agenda are the letter that the

16   defendant submitted at the end of trial yesterday, which

17   concerns AFD; Government Exhibit 820-224; Government Exhibit

18   806; the redaction issue; and the IRC chat issue.

19           I guess I put to you which of those needs to be

20   addressed this morning as opposed to later today.

21           MR. LOCKARD:  The issue with Government Exhibit

22   820-224 does not need to be addressed today, nor does the IRC

23   chat issue.  The issue with Government Exhibit 806 will need to

24   be -- 806 will come up today.

25           THE COURT:  All right.  I'm prepared to rule on that

M6sWsch1

1    in any event.  Bottom line is to the extent that the

2    application or argument being made at the present time is

3    admission of the top portion under Rule 106, the motion is

4    denied.  Looking at the unredacted version of the exhibit, it

5    seems clear that the different entries are precisely that --

6    different entries, which is to say that I don't read, to the

7    extent that the top is indeed something that Mr. Schulte

8    drafted for submission to Judge Crotty, I don't read the

9    portion that the government intends to offer as a continuation

10   of it.  It's separated by line.  It seems to be very different

11   in tone and substance, and it seems quite clear that it's not a

12   continuation of the top.

13        That conclusion is reinforced by Mr. Schulte's own

14   position before the first trial.  At ECF No. 282, he sought to

15   exclude the two portions of that page -- namely, the top, on

16   the grounds that it was work product; and the bottom, on the

17   grounds that it was irrelevant to the issues in trial.  I think

18   if I understand correctly, the government consented to redact

19   both and thus mooted the issue for purposes of Judge Crotty.

20   But the point for my purposes being that I think implicitly

21   Mr. Schulte, by taking that position, conceded that the middle

22   portion was different in kind than the top portion and not work

23   product.  So to argue otherwise now is inconsistent with the

24   position that he previously took and reinforces the conclusion

25   that it's not part of the same.  And for that reason, I don't

1            think that the top portion needs to be admitted out of fairness

2            or to put the middle portion in context.

3                      Again, to the extent that the application is to admit

4            the top under Rule 106 as part of the government's case, that

5            motion is denied.

6                      Anything else that we need to discuss this morning?

7                      MR. DENTON:  Your Honor, we're happy to try and take a

8            stab at the defendant's letter about AFD in an unclassified

9            context.  I'm not sure whether that will get us there, but we

10           thought in the interest of efficiency, we might try and address

11           it here?

12                     THE COURT:  Is that something that we do need to

13           address this morning before the next witness?

14                     MR. DENTON:  No, your Honor.

15                     THE COURT:  OK.  Let me see if we can get an update on

16           how many jurors we have, since that may bear on whether we --

17                     Well, while I get that, why don't you start by

18           addressing what can be addressed.

19                     MR. DENTON:  So, your Honor, just to separate out two

20           components of the defendant's application, or letter, first of

21           all, with respect to reports or work product, as we previously

22           reported to the Court, the government undertook significant

23           efforts to confirm that there were, in fact, no such reports,

24           other material, and we have done so.  So again, there's no sort

25           of exculpatory forensic report that we are aware of existing at

M6sWsch1

1    all.  So that's step 1.

2         Second, however, with respect to other reports

3    containing conclusions from the CIA, Judge Crotty reviewed the

4    entirety of the WikiLeaks task force report and made

5    determinations about which portions were relevant and helpful

6    under Section 4 of CIPA.  Those are what have been produced to

7    the defendant.  To the extent that there are other portions of

8    the report that are not, that reflects Judge Crotty's

9    conclusion in response to litigation about that subject.  So we

10   don't think there's any need to go any further with respect to

11   the paper record.

12        With respect to the testimony of the witness, the

13   defendant's attempts to sort of put pieces of this into the

14   record do not relieve him of his obligations under Section 5 to

15   give notice of classified information he intends to elicit.

16   The government has repeatedly reminded him that AFD, the

17   specifics of its work, remain classified.  The details of that

18   are so.

19        In responding to the defendant's allegations of *Brady*

20   violations, the government has never addressed sort of the

21   substance of the defendant's speculation about AFD or its work.

22   To the extent that he believes that sort of his inclusion of

23   these things in public dockets reflects some sort of

24   declassification, he's incorrect about that.  We have tried to

25   be judicious about what we have sought to sort of have redacted

1   or otherwise removed from the public docket when it came close

2   to the line.  But in any event, I think it's clear that nothing

3   in what the defendant has submitted suggests that this is

4   somehow an unclassified subject or otherwise outside the scope

5   of what he was obliged to give notice of, and that's

6   particularly true in context of the numerous notices and other

7   things the defendant has filed in this case.  He's aware of

8   this obligation and what it looks like and where the line is.

9   It's sort of beggar's belief at this point for him to be

10  suggesting that he didn't think he had to give notice of this.

11  Given that he failed to give Section 5 notice of his intention

12  to elicit classified information regarding AFD, we think that,

13  there, the Court is on solid ground in precluding the witness.

14          THE COURT:  Let me try and disentangle the different

15  pieces of this.

16          To the extent that Mr. Schulte renews his request for

17  the report, I accept the government's representation, that I've

18  previously accepted, that there is no such report.  And I think

19  that's the end of the matter.  If it turns out there is,

20  obviously, that's a big issue and we'll deal with it then.  But

21  I'm trusting the government that there is no such report.  So

22  that settles the third issue that he raises in his letter.

23          The first does not strike me -- I think when I

24  discussed this the other day, I said there were two scenarios

25  in which Mr. Schulte might, or put the burden on him to show

M6sWsch1

1     one of two things: one, that the particulars that he is seeking

2     to introduce are already part of the public record; or two,

3     that there is a *Brady* issue here -- that is, something

4     exculpatory.

5               To me, he has not carried his burden on No. 1.  The

6     citation that he makes to the record doesn't go beyond or goes

7     very little, if at all, beyond what I understood to be not

8     classified and part of the public record; that is to say, it

9     doesn't get into the particulars of what AFD is or did.  And so

10    I don't think he has persuaded -- he has not persuaded me that

11    there's any reason to question the government's classification

12    decisions or representations about those decisions.

13              I guess, and maybe it's hard to address this in this

14    setting -- I'm not sure -- but that leaves the middle point in

15    the letter; namely, a reference to a message that Agent

16    Evanchec sent.  I guess I wanted you to just address that a

17    little more specifically, Mr. Denton -- that is to say, whether

18    and to what extent that suggests that there is or was a finding

19    or something of that sort made by AFD that is inconsistent with

20    the government's theory that would potentially be exculpatory.

21    I think that's a separate question than whether the witness

22    that Mr. Schulte proposes to call, which is how this issue

23    arose or arises, can be called.  It's not clear to me that that

24    witness would be in a position to testify to the facts that are

25    set forth in here, to the extent that they are even

M6sWsch1

1    inconsistent with the government's theory.

2             All the jurors are here, so what I would propose is

3    let's leave it there for now, and you'll leave me in suspense

4    as to what your answer to that question is, but we'll circle

5    back to it later.

6             MR. DENTON:  That's fine, your Honor.

7             THE COURT:  Can we get the witness in and get the jury

8    up.

9             (Continued on next page)

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1              (Jury present)

2              THE COURT:  You may be seated.

3              Good morning.  Thank you, all, for being here on time

4    today.  And those of you who tested at home, thank you for

5    doing that.  Those of you who appeared and tested downstairs,

6    thank you for that.  I'm pleased to report that those who did

7    get tested downstairs, all of you are negative.  I trust that

8    those of you who tested at home are also negative.  So that's

9    very good news.

10             Later today, I may have an update for you on the

11   schedule, but in the meantime, we will pick up where we left

12   off, with the government's next witness.

13             Government, call your next witness.

14             MR. LOCKARD:  The government calls Jeremy Weber.

15   JEREMY WEBER,

16        called as a witness by the government,

17        having been duly sworn, testified as follows:

18             THE COURT:  Mr. Lockard, you may proceed.

19             MR. LOCKARD:  Thank you, your Honor.

20   DIRECT EXAMINATION

21   BY MR. LOCKARD:

22   Q.  Good morning, Mr. Weber.

23   A.  Good morning.

24   Q.  Mr. Weber, who is your employer?

25   A.  I work for the Central Intelligence Agency.

M6sWsch1                        Weber - Direct

1    Q.  When did you start working with the CIA?

2    A.  It would have been late November 2010.

3    Q.  What did you do before you started working with the CIA?

4    A.  I was active duty Marine Corps.

5    Q.  And what did your job responsibilities with the marines

6    include?

7    A.  Originally, I was an 0651, which is a data systems

8    technician, a system administrator within the Marine Corps.  I

9    did that for about two and a half years before joining the

10   Marine security guard program to guard embassies.

11   Q.  Mr. Weber, do you have an degree?

12   A.  Yes, I do.

13   Q.  In what subject matter is your degree?

14   A.  I have a degree in computing with a focus on computer

15   science.

16   Q.  Mr. Weber, turning to your time at the CIA, have you worked

17   in the Operations Support Branch?

18   A.  Yes, I have.

19   Q.  During what time period did you work in the Operations

20   Support Branch, or OSB?

21   A.  I worked in OSB when I started at the agency in 2010 all

22   the way until about summer of 2016.

23   Q.  What was your position in OSB during that time?

24   A.  I was a developer.

25   Q.  Do you see anyone in the courtroom today who worked with

M6sWsch1                        Weber - Direct

1    you in OSB?

2    A.   Yes, I do.

3    Q.   And can you indicate who that person is and where they are?

4    A.   Josh, sitting over there.

5              MR. LOCKARD:  I ask that the record reflect that

6    Mr. Weber has indicated the defendant.

7              THE COURT:  All right.  So noted.

8    BY MR. LOCKARD:

9    Q.   Mr. Weber, generally speaking, what did OSB do during the

10   time that you worked there?

11   A.   OSB was -- our job was to create capabilities for use in

12   cyber operations for the CIA, most specifically, focused on

13   human-enabled operations.

14   Q.   And when you talk about capabilities, can you just describe

15   what you mean in sort of layperson's terms?

16   A.   In layperson's terms, what these are often referred to is

17   hacking tools, but they were tools for getting information off

18   of computer networks.

19   Q.   And without getting into any specifics, what do you mean by

20   human-enabled operations?

21   A.   So, human-enabled operation would be an operation where a

22   human is willing to touch a computer or get close to a computer

23   for us.

24   Q.   Generally speaking, what types of targets did OSB develop

25   cyber tools for?

1    A.   OSB, being in the CIA, all of our targets were at the time

2    focused on either foreign intelligence, so collection from

3    foreign governments, or the counterterrorism mission.

4    Q.   And in OSB in particular, during your time there, was there

5    a category of targets that OSB focused on?

6    A.   At the time we were heavily involved with the

7    counterterrorism mission, so we were heavily focused on

8    terrorist organizations.

9    Q.   You've talked about operations.  Did OSB developers deploy

10   the tools that you developed?

11   A.   No.

12   Q.   Who deployed the tools?

13   A.   We had a mission partner within, a mission partner in COG

14   that was often responsible for either deploying the tools or

15   interacting with the asset that would deploy the tool.

16          MR. LOCKARD:  Ms. Cooper, could we please pull up

17   Government Exhibit 89 for Mr. Weber.

18   Q.   Just to situate ourselves organizationally, where is the

19   branch that you worked in from 2010 to 2016?

20   A.   I'm in the Operations Support Branch.

21        Do you want me to circle it?

22   Q.   Is that the box in the lower left corner?

23   A.   Correct.

24   Q.   OK.  And that is part of the Engineering and Development

25   Group?

M6sWsch1                        Weber - Direct

1    A.   That is correct.

2    Q.   So you mentioned COG.  Is COG a part of the Engineering and

3    Development Group?

4    A.   No, it's not.

5    Q.   Is that a separate group in CCI?

6    A.   Correct.

7    Q.   And did OSB have sister development branches?

8    A.   Yes, it did.

9    Q.   And did they have slightly different focuses in their

10   development projects?

11   A.   Correct.

12           MR. LOCKARD:  Thank you, Ms. Cooper.

13   Q.   Mr. Weber, during your time in OSB, did OSB and its sister

14   development branches use a particular computer network to

15   develop those foreign intelligence cyber tools?

16   A.   Yes, we did.

17   Q.   Did that network have a name?

18   A.   Yes, it did.

19   Q.   And what was that name?

20   A.   DevLAN.

21   Q.   Generally speaking, who had access to DevLAN during your

22   time at OSB?

23   A.   It would have been officers within the Engineering

24   Development Group, either -- primarily it was the developers

25   within AED, but some others that had support roles within EDG

M6sWsch1                           Weber - Direct

1    also had access to the network.

2    Q.  Did there come a time when you and the other developers in

3    AED stopped using DevLAN?

4    A.  Yes.

5    Q.  When was that?

6    A.  It would have been on March 7, 2017, when the Vault 7 leaks

7    hit.

8    Q.  How did you learn about the Vault 7 release?

9    A.  I was -- I was called in to the office.  I was supposed to

10   be heading to an offsite that day, but was called in to the

11   office, told to get in as quickly as possible, and was brought

12   to a conference room, and there was a printout of what was

13   published that day put in front of me.

14   Q.  And did you review the contents that had been made

15   available?

16   A.  Yes.

17   Q.  Did you recognize it?

18   A.  Yes, I did.

19   Q.  What was it?

20   A.  It was -- it was the -- we had a suite of tools, and under

21   that suite was a product called Confluence, which was a wiki

22   that was used by AED.  It appeared to be the information pulled

23   from there.

24   Q.  Were there additional releases of DevLAN data after March

25   7, 2017?

1    A.   Yes, there was.

2    Q.   And did you review those as well?

3    A.   Often, yes.

4    Q.   And what was the purpose of your reviewing those materials?

5    A.   We were focused on what the scope of the damage was for

6    what was coming out.  So whenever something was released, we

7    would look through to see what was in it and then make

8    recommendations about what -- what damage that would do to

9    operations and capabilities within CCI.

10   Q.   What effect did the WikiLeaks releases have on the work

11   that you had done at OSB?

12   A.   It was extremely damaging.  Everything -- everything that

13   we wrote was essentially labeled as no longer to be used, and

14   we had to start from scratch.

15   Q.   And what effect did that have on your ability to deploy

16   tools in future operations?

17             MR. SCHULTE:  Objection.

18             THE COURT:  Overruled.

19   A.   The -- again, we -- we had to rewrite a significant amount

20   of stuff.  Some stuff we were able to rewrite.  Other things

21   were a loss of capability that we didn't get back.  It was

22   very -- it was very broad in the amount of, amount of tools

23   that were out, and it was a case-by-case basis on what we were

24   able to recover and how long it took us to recover.

25   Q.   Now, you said that you stopped using DevLAN on March 7,

M6sWsch1                          Weber - Direct

1    2017?

2    A.   Yes.

3    Q.   What effect did the WikiLeaks releases have on developers'

4    ability to actually do development work?

5    A.   DevLAN ceased to exist on March 7.  Everybody -- everybody

6    was not allowed to touch their computers anymore, and we didn't

7    have the physical tools we needed to be able to do our job.

8        Anthony, at the time, in that first week, worked with our

9    logistics team to try and just find laptops, whatever, to be

10   able to get developers writing code again.

11   Q.   So you referred to Anthony.  What was Anthony's position at

12   the time?

13   A.   Anthony was chief of the Applied Engineering Division at

14   the time.

15   Q.   What happened to the DevLAN network after March 7, 2017?

16             MR. SCHULTE:  Objection.

17             THE COURT:  Overruled.

18             To the extent that you didn't already answer it, you

19   may answer.

20             THE WITNESS:  OK.

21   A.   The DevLAN, shortly after March 7 is when the FBI arrived.

22   And the FBI began collecting every piece of equipment that was

23   attached to DevLAN, and it was removed, removed from the

24   vaults, never to be seen again, essentially.

25   Q.   Mr. Weber, you talked about the effect the WikiLeaks

M6sWsch1                       Weber - Direct

1    releases had on the tools --

2             MR. SCHULTE:  Objection.  He's testifying.

3             THE COURT:  Overruled.

4    Q.  -- the tools that AED had developed.  What, if any, effect

5    did the release have on past operations?

6    A.  Past operations were put at significant risk.  Either in

7    terms of loss of access for, if we had leave-behind capability

8    left on the network or potentially an attribution statement

9    for, could come into effect if -- if the capabilities that were

10   used in operation were caught and potentially then tied to CIA

11   activity.

12   Q.  You referred to something you called an attribution.

13   Again, without getting into any specifics, what do you mean by

14   attribution in this context?

15   A.  So, attribution is one of the main concerns that developers

16   within EDG have to take into account for when we are creating

17   these capabilities.  The CIA operates in secret.  We do not

18   want our activities tied back to the CIA or the U.S.

19   government.

20   Q.  And you said that OSB worked on human-assisted operations.

21             MR. SCHULTE:  Objection.

22             THE COURT:  Overruled.

23   Q.  Again, without getting into any specifics, what are the

24   risks of attribution in a human-assisted operation?

25   A.  In a human-assisted operation, the risk of attribution

1    would be that that -- that human asset is labeled as a spy for

2    the CIA.

3    Q.  And what risk does that pose for people who are involved in

4    operations targeting terrorist organizations?

5             MR. SCHULTE:  Objection.

6             THE COURT:  Overruled.

7    A.  For a terrorist organization, I think the asset's main fear

8    would be to be executed for being a CIA spy.

9    Q.  Mr. Weber, you described the information as having come

10   from Confluence?

11   A.  Correct.

12   Q.  When you reviewed the information that was released by

13   WikiLeaks, where did you review it?

14   A.  I reviewed it within vaults in the CCI office within our

15   building.

16   Q.  And why did you review the information inside the CCI

17   office in vaults?

18   A.  The information was classified and should only be processed

19   within a secure facility.

20   Q.  So if the data had already been released on WikiLeaks, why

21   would it remain classified and be reviewed in a classified

22   setting?

23            MR. SCHULTE:  Objection.

24            THE COURT:  Overruled.

25   A.  The information was still considered classified.  Even

1    though it had been leaked by WikiLeaks, the U.S. government

2    wasn't making any statements about ownership of that or if it

3    was valid information.

4    Q.   And Mr. Weber, other than in connection with this case,

5    have you ever spoken publicly about Vault 7?

6    A.   No, I have not.

7    Q.   Turning back to development, again, you mentioned

8    Confluence.  What were the programs that you and the other

9    developers used for your work on cyber tools?

10   A.   So, there's a lot of commercially available software that

11   we use.  Specifically, we use the Atlassian tool suite, which

12   covered Confluence, Bamboo, Jira, and at the time it was

13   referred to as Stash.  Atlassian has renamed the product to

14   Bitbucket.

15   Q.   I'd like to talk for a minute about administration.  So who

16   administered the DevLAN network itself?

17   A.   The EDG had a dedicated system administration team in the

18   Infrastructure Support Branch, ISB.

19   Q.   And was ISB, was that part of the Applied Engineering

20   Division?

21   A.   No, it was not.

22   Q.   You testified that you have a background in systems

23   administration?

24   A.   That's correct.

25   Q.   Is it good practice for the administrators of the system to

M6sWsch1                         Weber - Direct

1    be separate from the users?

2    A.   It very much is.

3    Q.   Why is that?

4    A.   Partially specialization.  System administration is a

5    specific job.  You want people that are trained to do that job

6    doing it.  But also, due to the level of access system

7    administrators have, you want to make sure that they are

8    separate from the general user base.

9    Q.   And what is the significance of that in a network like

10   DevLAN?

11   A.   So, for a network like DevLAN, which processes classified

12   information, there is a lot of need to know that even though a

13   system administrator could conceivably access it, they

14   shouldn't access that information.

15   Q.   Now, who administered the Atlassian programs?

16   A.   It would have been developers within AED.

17   Q.   So how did it come about that those programs were

18   administered by developers in AED instead of by ISB, the group

19   that did the systems administration?

20   A.   I forget the year, but originally, AED was tasked to find a

21   replacement for the tools we were using at the time.  A team of

22   developers got together to assess what would be best for our

23   work flow.  We decided on the Atlassian tool suite and went to

24   ISB and said please install this for us.  ISB didn't have the

25   free cycles nor the technical experience.  They were primarily

M6sWsch1                         Weber - Direct

1    a Windows development -- Windows support shop, whereas the

2    Atlassian tool suite was meant to be developed -- meant to be

3    run on Linux.

4         For those two reasons, ISB felt they wouldn't be able to

5    take it on.  And Patrick, one of the developers within AED,

6    volunteered to be the ones that did the initial install and

7    setup, with the hope of eventually passing it over to ISB.

8                THE COURT:  What did you mean by free cycles?

9                THE WITNESS:  I apologize.  Free cycles, he had the

10   extra time and the expertise to be able to do that.

11   BY MR. LOCKARD:

12   Q.  So was having developers administer the Atlassian programs

13   intended to be the permanent solution?

14   A.  No, it was not.

15   Q.  And again, what was intended?

16   A.  The intention was for it to eventually be passed over to

17   ISB.  It was something that we frequently brought up.

18   Q.  So which developers in AED held Atlassian administrative

19   roles?

20   A.  Originally, the Atlassian administration was Patrick's job,

21   but when Patrick was selected for an overseas position, I

22   volunteered to assume the responsibilities, and I asked for

23   Josh to -- to help me out with it.  So it was the three of us.

24   Q.  And why did you ask the defendant to help you with

25   administering the Atlassian programs?

M6sWsch1                         Weber - Direct

1    A.   My Windows -- my background was as a Windows system

2    administrator as well as a Windows developer.  I had very

3    limited Linux experience, and Josh had more Linux experience.

4    So I asked him to help me out on the project.

5    Q.   And why was Mr. Schulte's Linux experience important?

6    A.   The Atlassian products were installed on Linux

7    infrastructure.

8    Q.   What were the responsibilities of the Atlassian

9    administrators?

10   A.   Generally speaking, it was to keep the lights on for the

11   products.  We would apply patches.  We would make sure that

12   they stayed up and running.  If updates came out, we would

13   install those to give new features to the developers.  And

14   occasionally, if there were issues with the permissions that

15   were assigned to certain projects, we might be called to fix

16   those.

17   Q.   You just mentioned permissions.  What are permissions?

18   A.   Permissions are, in this context, were Atlassian's means

19   for limiting access to the projects that you were allowed to

20   see.  So a standard user would not be able to see everything

21   that was in Stash or Confluence.

22   Q.   And is that different for an Atlassian administrator?

23   A.   Yes.

24   Q.   How is that different?

25   A.   An Atlassian administrator had the ability to elevate the

1    privileges up to the admin level and would be able to see

2    everything within those products.

3    Q.  As an Atlassian administrator, how did you know when you

4    had the authority to use your administrator permissions?

5    A.  The -- we had well-defined reasons for having to use it --

6    again, primarily for the care and maintenance of that as well

7    as if somebody requested that we fix something for them.  We --

8    we, as agency officers, had very routine training, explaining

9    the idea of, you know, accessing only information that you're

10   authorized to see and making sure that you don't abuse the

11   privileges that a security clearance, the level of information

12   that a security clearance could conceivably give you access to.

13   Q.  As an Atlassian administrator, how did you know when you

14   were exercising those administrator privileges?

15   A.  You -- you would have to elevate your privileges.  For

16   Atlassian, when you would log in, when you would log in to the

17   website, you would, by default, log in as a standard user.

18   Atlassian administrators would've had, if I recall correctly,

19   in the upper right-hand corner, there was a little icon that

20   you could click, and it would say log in as an administrator,

21   and you would be re-prompted for your password to -- to then be

22   able to do the things that you would need to do as an

23   administrator.

24   Q.  And once you elevated your privileges, would they remain

25   elevated throughout the rest of your session?

1    A.   Until you closed out that session by either closing out the

2    browser, and I believe there was a time-out as well.

3    Q.   Did the developers who administered the Atlassian programs

4    get higher pay?

5    A.   No, they -- we did not.

6    Q.   Did the developers who administered the Atlassian programs

7    have a higher status within AED?

8    A.   No.

9         MR. LOCKARD:   Ms. Cooper, if we could pull up

10   Government Exhibit 1251, please.

11   Q.   Mr. Weber, do you recognize what's displayed here?

12   A.   Yes, I do.

13   Q.   Is this an accurate representation of the DevLAN network as

14   it existed during your time at OSB?

15   A.   Yes, it is.

16   Q.   So again, we talked about DevLAN being administered by ISB.

17   What are the components of the DevLAN network that ISB was

18   responsible for?

19   A.   The ISB was responsible for everything within DevLAN, but

20   specifically, they were responsible for the stuff that you see

21   on the bottom half of this in blue, the DevLAN users box and

22   NetApp file server box as well as the stuff in the middle

23   there, the DevLAN, the network switch, the firewall.

24   Q.   Looking up at the top half of that box, which branch, so to

25   speak, owned the Stash server?

M6sWsch1                          Weber - Direct

1    A.   ISB owned the Stash server.

2    Q.   And who had administrative responsibilities for

3    administering the Stash server?

4    A.   That would have been the Atlassian administrators,

5    originally Patrick and then Josh and I.

6    Q.   And why was that if that's an ISB server?

7    A.   Again, ISB -- ISB didn't have the time to be able to

8    administer that, nor did they have the experience on doing it.

9    So they -- they relied on us to be able to maintain the server

10   and keep it up and running.

11   Q.   You've described Confluence briefly.  Can you also give us

12   a brief description of Stash and what its use is?

13   A.   Yes.  So, Stash was meant for code collaboration.

14   Everything a software developer does essentially boils down to

15   writing -- writing computer code.  Stash was a way for not only

16   us to back up the source code that we created, but it was meant

17   to be a means for us to collaborate with each other.  You could

18   view the source code.  We would do code reviews often.  And

19   this was a way that you could comment on other people's work to

20   highlight potential tradecraft issues or errors that were in

21   somebody else's code.

22   Q.   How did the concept of permissions apply to Stash?

23   A.   So, Stash -- Stash was -- each branch and the project

24   owners for the projects that were in Stash would make

25   permission decisions on how -- how much visibility that project

M6sWsch1                         Weber - Direct

1     would have.  Some projects were open for everybody within AED.

2     Some projects might be limited to one or two users being the

3     only ones that can access that project.

4     Q.   And can you describe briefly what Crowd did?

5     A.   Crowd was a simple tool that -- its job was to translate --

6     translate Active Directory permissions, which Active Directory

7     was the main way DevLAN used to authenticate users, and Stash

8     had its own means of authentication.  So rather than have users

9     have different -- different usernames and passwords, Crowd's

10    job was to authenticate Stash users against Active Directory.

11    Q.   And that was to pass permissions from the Active Directory

12    to the Stash tools?

13    A.   Not -- Stash was responsible for the permissions.  All

14    Crowd did was authenticate a user.  So when I would log in with

15    my username and password, rather than Stash figure out if that

16    was an accurate username and password, Crowd would pass that

17    over to Active Directory to say yes, this is Jeremy, and then

18    apply the appropriate permissions that were stored within

19    Stash.

20    Q.   Let's turn to the box to the left under the Stash server,

21    the ESXi server.

22    A.   OK.

23    Q.   Which branch, so to speak, owned the ESXi server?

24    A.   This ESXi server was owned by OSB.

25    Q.   And who administered the ESXi server?

1    A.   It was some developers within OSB, Josh and I.  And I

2    believe Frank and Matt were also administers of the ESXi

3    server, but primarily Josh and I.

4    Q.   Was Confluence used only by OSB?

5    A.   No.

6    Q.   Why was Confluence hosted on the OSB server?

7    A.   The ESXi server was relatively new.  We had just purchased

8    it -- we being OSB.  So it -- it had enough CPU and RAM to be

9    able to do, run a lot of virtual machines.  At the time ISB

10   didn't have enough -- enough servers to be able to run

11   Confluence and Bamboo as well.  Pretty much the only thing that

12   they had the spare computers for was to run the Stash server.

13   So again, a temporary solution was let's deploy this on OSB's

14   ESXi server as a temporary home.

15   Q.   If we could just briefly address some of the things that

16   were running on the ESXi server.  How did the developers use

17   development VMs?

18   A.   So, the development VMs could meet a broad range of use

19   scenarios.  Part of it was some tools were rarely used,

20   commercially available tools were rarely used, but

21   occasionally, you would need to leverage them.  So rather than

22   having to install and keep a copy of it on your local computer,

23   we had some development VMs that could be leveraged by users to

24   be able to go and use those tools.

25        Other scenarios would be as test targets.  When we create

M6sWsch1                          Weber - Direct

1    capabilities, we want to test it against the most -- most

2    accurate representation we have to the target environment.  So

3    those development VMs would be set up in a similar way, you

4    know, the type of OS that was installed, operating system; the

5    language pack, things like that.  So they would test things as

6    well as just other -- other, like, things just to ease our

7    development process.

8    Q.  Turning back to the ESXi administrators, what authorities

9    did ESXi administrators have over the programs that were hosted

10   on that server?

11   A.  So, an ESXi administrator had the ability to create VMs,

12   delete VMs, take snapshots of VMs, things like that.  So they

13   could -- they could essentially handle where, like, where the

14   VMs were set up, but being an ESXi administrator didn't give

15   you access to the VMs themselves.  That would be a -- a

16   separate set of permissions.

17   Q.  And in your role as an administrator, did you create

18   snapshots of VMs?

19   A.  Yes.

20   Q.  And generally speaking, for what purpose would you do that?

21   A.  So, a snapshot is meant to be a way to revert changes back

22   to a previous state.  Most often, this was used in the test

23   environment.  We would -- we would set up the -- we would set

24   up the test VM into, you know, be, like I said, a

25   representative environment.  And then we would test our tool

M6sWsch1                        Weber - Direct

1    against it.  You would test often, so whenever you finished

2    testing, you would often revert back to a snapshot so that you

3    reset the VM to a clean state.

4        Also, when it came to doing system administration tasks of

5    things like Confluence and Bamboo, we would often take a

6    snapshot so that if we made a mistake during the installation

7    and update, we could revert back and try again.

8    Q.  And in the development scenario that you described, where a

9    snapshot is taken and then tools are tested, what is the effect

10   on the changes that had happened to the VM during testing when

11   you revert the virtual machine back to the snapshot?

12   A.  Everything within the VM, any changes that occurred, would

13   go back to the state in the snapshot.

14   Q.  In your role as an ESXi administrator, did you ever take a

15   snapshot of the Confluence VM?

16   A.  Yes.

17   Q.  How many times?

18   A.  A handful of times.  I'm not sure exactly how many times.

19   But again, general practice was if we were making changes, we

20   would take a snapshot prior to making those changes.

21   Q.  And then just to round out this box, can you give us a

22   brief description of what Bamboo does?

23   A.  Yes.  So, Bamboo -- Bamboo is meant to support a software

24   development concept of continuous integration, the idea being

25   that during the development process, rather than wait for your

1  tool to be fully complete, to test your tool, you would have an

2  iterative approach to development -- so make a change, test the

3  change, make the change, test the change.  That way, if you

4  make a mistake that breaks something, you find out about it

5  early in the development cycle rather than late.  Bamboo was a

6  means to automate the testing of capabilities.

7  Q.  And so, Mr. Weber, you were an Atlassian administrator?

8  A.  That's correct.

9  Q.  As well as an ESXi administrator?

10  A.  For the OSB server.

11  Q.  For the OSB server.  What is different about those two

12  administrative roles, especially here in this box, where

13  Confluence is on the ESXi server?

14  A.  So, again, the ESXi server administration would allow us to

15  make changes to the server as well as -- again, you could

16  create, delete VMs, modify, like, how much CPU is dedicated to

17  it, things of that nature.  It did not give you any ability to

18  access the VM itself.  That's where the Atlassian administrator

19  privileges came into play.  So outside of the VM was the ESXi

20  administrative duties.  Inside the VM was the Atlassian

21  administrative duties.

22  Q.  In your experience as a system administrator and as an

23  Atlassian administrator, are you familiar with the concept of

24  log files?

25  A.  Yes, I am.

M6sWsch1                          Weber - Direct

1   Q.   Broadly speaking, what are log files?

2   A.   Log files are a means to log -- sorry for using the word in

3   the definition, but to write out -- write out system status

4   messages or changes or error messages, to be referenced later.

5   So in software development, we would often have very robust

6   logging that would say what the status was of the program that

7   was running, like, what, you know, certain variables were set

8   to, so that if we were trying to debug something, we could know

9   potentially where something went wrong.

10       In terms of system administration, logs could be anything

11   from who accessed, who accessed or logged in to something,

12   security events, error events.  The idea is it's a means to

13   help troubleshoot any issues that could come up with the

14   running of a system.

15   Q.   As a systems administrator, would you ever delete log

16   files?

17   A.   Not -- not individual log files.  Potentially, the more

18   likely scenario is you would have -- you would have a policy

19   of, like, either a maximum file size for logs or a maximum age.

20   So -- so generally speaking, a system administrator's not going

21   to care about log files that are five years old.  So you might

22   have something that once a log file gets to a certain age,

23   it -- it falls off the back end, to make sure that you don't

24   run out of space on the system.

25   Q.   You mentioned a hypothetical five-year time period.  What

1      time period of log files would be the most relevant to a

2      systems administrator?

3      A.   The most recent ones.

4      Q.   Mr. Weber, if we could just turn to the bottom right-hand

5      corner of the exhibit, 1251, there's a server labeled Hickok.

6      Can you describe what the function of that server was?

7      A.   So, Hickok was what we refer to as a DMZ.  So, Hickok

8      existed between DevLAN, EDG's network, as well as COG's mission

9      network.  COG was our main mission partner, and there was some

10     information that had to be exchanged back and forth between the

11     two networks to ensure the speed of the mission.  So Hickok was

12     meant to facilitate the transfer of information that was

13     authorized to go between the two, while remaining -- helping

14     ensure the system integrity of the systems otherwise.

15     Q.   I think you referred to a DMZ?

16     A.   Yes.

17     Q.   What is a DMZ in a network setting?

18     A.   So, a DMZ is a, is a zone that exists outside of your main

19     portion of the network, where the idea is that there is a

20     broader access to that area and might have different

21     permissions and rules applied to it.

22     Q.   When you say broader access, a broader access on which side

23     of the fence?

24     A.   So, in -- in the standard world, a DMZ often would be

25     where, like, a web server exists, where users are accessing it.

1    In this specific sense, we're talking about the broader sense

2    being the COG mission network and users on the COG mission

3    network being able to access it.

4    Q.   And then what is the purpose of the firewalls represented

5    by those two brick squares on either side of the DMZ?

6    A.   So, a firewall's purpose is to ensure allowed traffic goes

7    through and disallowed traffic is blocked.  So its job was the

8    protection of -- protection of the respective networks.

9    Q.   Let's look at the bottom right box, the NetApp file server.

10   A.   OK.

11   Q.   Who administered that server?

12   A.   That would be ISB.

13   Q.   There's a folder on there called Altabackups?

14   A.   Correct.

15   Q.   What was that folder used for?

16   A.   So, during -- during Josh and I's tenure as Atlassian

17   administrators, we needed to update where the products were

18   backed up to.  Altabackup was created by ISB to enable that

19   backup.

20   Q.   Who asked ISB to set up that folder?

21   A.   I did.

22   Q.   And who was responsible for permissions on that folder?

23   A.   ISB.

24   Q.   During your time in OSB, did you access the Altabackups

25   folder?

M6sWsch1                          Weber - Direct

1   A.   Yes, I did.

2   Q.   How many times?

3   A.   A handful of times.  At most, probably once or twice,

4   mainly -- mainly just to validate that files were being written

5   to that folder when we set up the backups.

6   Q.   And when the backup folder was set up, who was responsible

7   for ensuring that the backups were copied to the new backup

8   location?

9   A.   Josh and I were the responsible party.  Josh was the one

10  who created the script that would back -- or I should say

11  modify the script that would back the information up to that

12  location.

13  Q.   How would you access the Altabackup folder?

14  A.   So, the ways I access it were via a VM.  We would use a

15  Linux command called mount, which would then go and connect the

16  Altabackup to that Linux VM so that you could navigate to it.

17          (Continued on next page)

18

19

20

21

22

23

24

25

M6S5sch2                        Weber - Direct

1    BY MR. LOCKARD:

2    Q.  And from what Linux VM would you execute that mount

3    command?

4    A.   So, I had a Linux VM on my machine.  I believe Josh had his

5    own.  And then, most importantly, the Confluence VM, the -- the

6    Confluence VM and the Stash machine had that folder mounted so

7    that they could write to it.

8    Q.  Can you just explain the relationship between the VM you

9    had on your DevLAN station and the Confluence VM that had the

10   Alta backups mounted?

11   A.   The Confluence VM that had that mounted was the VM that

12   Confluence was actually running in so the script was writing to

13   a remote location and so that location had to be accessible to

14   it.

15   Q.  How did you learn how to use a mount command?

16   A.   Josh would often help me with it.

17   Q.  So you have touched a little bit on your and Mr. Schulte's

18   roles as Atlassian administrators.  During what time was

19   Mr. Schulte a developer in OSB?

20   A.   So roughly -- roughly from the time that I started in OSB

21   through -- through 2016, I believe, or late 2015 I think is his

22   OSB time.

23   Q.  Did you work near each other?

24   A.   Yes.

25   Q.  Where were your desks located?

M6S5sch2                        Weber - Direct

1    A.   We are talking about a five-year period here so desks

2    changed.   At the beginning, Josh and I were in different aisles

3    but towards the end Josh sat next to me.

4    Q.   And how would you describe your relationship with

5    Mr. Schulte in the first few years of your working together?

6    A.   We had a good relationship.   I would have considered him a

7    friend.   I often reached out to him to collaborate on projects,

8    get advice on how we should go about doing stuff.   I think we

9    had both a close working relationship as well as being friends

10   outside of work.

11   Q.   Did you, from time to time, work on projects together?

12   A.   Yes.

13   Q.   Did you, from time to time, invite Mr. Schulte to work on

14   projects with you?

15   A.   Yes.

16   Q.   Did there come a time when your friendly relationship

17   changed?

18   A.   Yes.

19   Q.   Did something cause that change?

20   A.   Yes.

21   Q.   What caused that change?

22   A.   So a new developer was hired into OSB; Amol.   When Amol

23   started working with us his relationship and Josh's, it slowly

24   but steadily went downhill and became more adversarial with

25   each other.   The drama that that was causing, you know, made

1     me -- I was getting tired of, you know, what Josh was doing and

2     so that caused me not to -- both, not want to work with him as

3     much but also not hang out with him as much.

4     Q.   Did there come a time that you learned that Mr. Schulte

5     made allegations about Amol?

6     A.   Yes.

7     Q.   And how did you learn that?

8     A.   So I don't remember the specifics of how I learned about

9     it, like the initial thing, but Josh had made an accusation

10    that Amol had threatened his life and I was named in that

11    accusation, and because of that I had to make an official

12    statement -- an official statement regarding Josh's statement

13    as well as Amol asked me to eventually go to trial as a witness

14    for him.  So I don't know specifically how I learned about it,

15    if it was through, you know, just rumor of the day's events or

16    if it was security that told me originally, but definitely

17    eventually through being officially pulled in.

18              MR. LOCKARD:  Ms. Cooper, can we pull up Government

19    Exhibit 1020?

20    Q.   Mr. Weber, have you had a chance to review this e-mail

21    prior to your testimony today?

22    A.   Yes, I have.

23    Q.   Does it reflect some of the allegations you learned about

24    during your time at OSB?

25    A.   Yes, it does.

M6S5sch2                         Weber - Direct

1              MR. LOCKARD:  Can we focus in on the second paragraph?

2    Q.  So in the first sentence where it says Amol is very

3    derogatory and abusive to everyone around him, what was your

4    experience with Amol?

5    A.  Amol and I got along quite well.  I did not feel he was

6    ever abusive to me.  He was somebody I considered a friend.

7              MR. LOCKARD:  If we could pull that down and go to the

8    fourth paragraph?

9    Q.  Mr. Weber, you said your name had been brought into the

10   allegations?

11   A.  Yes.

12   Q.  Does this reflect the way in which your name was brought

13   in?

14   A.  This was the allegation that pulled me into it.

15   Q.  If we could start with the first couple sentences of this

16   paragraph where it reads:  No one is immune from Amol insults;

17   even people's wives.  Amol has gone so far as to directly

18   insult Jeremy Weber's wife and father-in-law.  He has directly

19   called them both dumbasses and idiots for their investment

20   choice in the G-Fund.

21        Do you agree with that characterization?

22   A.  No, I don't.

23   Q.  What was your experience?

24   A.  Amol and I would occasionally talk investments and

25   investment strategies.  At the time my retirement fund was

M6S5sch2                          Weber - Direct

1    entirely invested in the G-Fund which is the lowest growth

2    fund, typically, because it is an investment in bonds.  Amol

3    felt that that was a very poor investment choice but it was

4    something my wife -- and my wife based on her experience with

5    my father-in-law -- was very fervent about.  So Amol would

6    often refer to the decision as dumb but I -- he wouldn't call

7    my wife dumb.

8    Q.   And then going to the next sentence:  Despite multiple

9    attempts by Jerry to dissuade and stop this outrageous

10   behavior, Amol will still discuss this topic and laugh in

11   Jeremy's face.

12        Do you agree with that characterization?

13   A.   No, I don't.

14   Q.   Did Amol ever laugh in your face?

15   A.   No.

16   Q.   Did you ever attempt to dissuade Amol from this outrageous

17   behavior?

18   A.   I don't believe so.  I tended to agree that the decision to

19   invest in the G-Fund was dumb.  I often brought it up with my

20   wife as well, but I was more concerned with having a happy

21   marriage than having a more secure retirement so it wasn't

22   something that I would often dissuade or wouldn't ask Amol to

23   stop talking about.

24             MR. LOCKARD:  Thank you, Ms. Cooper.  If we could

25   please pull up Government Exhibit 1038, and specifically to

M6S5sch2                          Weber – Direct

1   page 4?

2   Q.   Mr. Weber, do you recognize that handwriting?

3   A.   Yes, I do.

4   Q.   And if you look in the bottom right-hand corner -- I'm

5   sorry.  Whose handwriting is it?

6   A.   Joshua Schulte.

7   Q.   Have you seen his handwriting in the course of your working

8   with him at OSB?

9   A.   Yes.  I often had to try and decipher what he had written

10   out.

11   Q.   And what is the date in the bottom right-hand corner?

12   A.   This would be March 17th, 2016, I believe.

13          MR. LOCKARD:   And if we can turn to the next page?

14   Thank you.

15   Q.   Is this a typewritten version of the same statement?

16   A.   Yes, it is.

17   Q.   So again, are these allegations that you learned of while

18   you were in OSB?

19   A.   Yes, they are.

20   Q.   So if we can look at the second paragraph and turning, in

21   particular, to the last sentence where it says "this" -- I

22   think referring to the sentence right before that -- infuriated

23   Amol because usually people do not respond to his bullying or

24   attempt to fight back.

25          Do you agree with that statement?

1    A.   No, I don't.

2    Q.   Why not?

3    A.   I never saw Amol as someone who was bullying people in the

4    office, and in the times where it was more in the nature of

5    good-hearted ribbing back and forth between officers people

6    were more than willing to, you know, rib Amol back, so.

7    Q.   So in the third paragraph, starting the second sentence

8    there is a description of an event involving Amol coming

9    towards Mr. Schulte and making statements towards him.

10   A.   OK.

11   Q.   Were you present for any event like that?

12   A.   I don't believe so.

13   Q.   Then turning to the last sentence where it says I was

14   afraid that he might stab or assault me in some way; I was

15   frightened and very concerned, especially based on his

16   behavior.

17            MR. SCHULTE:  Objection.  They should call Amol if

18   they want this out.

19            THE COURT:  Mr. Schulte, please.  Hang on one second.

20   I don't know what the question is yet.

21            Finish your question, Mr. Lockard.

22   BY MR. LOCKARD:

23   Q.   Mr. Weber, did Mr. Schulte ever express fear of Amol to

24   you?

25   A.   No, he did not.

M6S5sch2                         Weber – Direct

1    Q.   How did the allegations we just discussed, how did that

2    affect your relationship with Mr. Schulte?

3    A.   It was the final straw, so to speak.  At this point I was

4    just fully done with my interactions with him.  I just didn't

5    want to deal with him anymore either at work or outside of

6    work.

7    Q.   You mentioned a court proceeding earlier?

8    A.   Yes.

9    Q.   Generally, what was the nature of that court proceeding?

10   A.   So Josh took out a restraining order against Amol and Amol

11   was challenging that restraining order and requested that

12   myself and a few others testify on his behalf.

13   Q.   And did you agree to do that?

14   A.   Yes, I did.

15   Q.   Did you testify?

16   A.   No, I did not.

17   Q.   Why not?

18   A.   There was -- the restraining order was filed in the wrong

19   jurisdiction and was thrown out based on that, and to my

20   knowledge was never, like, reapplied for so my testimony wasn't

21   needed.

22        MR. LOCKARD:  Thank you, Ms. Cooper.  We can take this

23   down.

24   Q.   So what effect did that situation have on staffing in the

25   Operation Support Branch?

1    A.  So originally the -- Josh and Amol were requested to move

2    desks so they weren't sitting physically next to each other,

3    but eventually it was decided that that move wasn't far enough

4    and both Amol and Josh were reassigned to different branches

5    within AED.

6              MR. LOCKARD:  Could we please look at Government

7    Exhibit 89 again?

8    Q.  Starting with Amol, to which branch was he moved?

9    A.  Amol was moved to MDB.

10   Q.  And to which branch was Mr. Schulte moved?

11   A.  Josh was moved to RDB.

12   Q.  Did you consider the move to RDB as a demotion?

13   A.  No.

14   Q.  Why not?

15   A.  All of the branches were peers to each other.  They

16   simply -- simply had different mission focuses.  RDB and OSB

17   had a very close relationship because the mission focus often

18   overlapped and, quite frankly, RDB was also a collection of

19   some of our most senior officers at the time.

20   Q.  So did you learn of any decisions about Mr. Schulte's

21   projects within OSB resulting from this move?

22   A.  Yes.

23   Q.  And what did you learn?

24   A.  So at any time somebody moves branches for the most part

25   it's decided if any project should go with them.  Again, the

M6S5sch2                        Weber - Direct

1    different branches have different mission focuses so some

2    tools, even though they were originally written by somebody

3    else, might remain behind.  So there was discussion about

4    Josh's projects, about which ones should go and which ones

5    should stay based on mission need.

6    Q.  And who was involved in those discussions, from your

7    perspective, that you were involved in?

8    A.  So it was mainly a leadership discussion at the branch

9    level so RDB and OSB's branch chief, along with Anthony at the

10   division level, but developers' input would have been sought.

11   Assignment of projects often was the branch chief reaching out

12   and finding out who was interested in taking over a project or

13   who had the cycles -- the free time -- to be able to work on

14   said project but primarily it would have been a

15   branch-leadership-and-above discussion.

16   Q.  And what was the name of the head of the OSB branch at the

17   time?

18   A.  Sean.

19   Q.  So what was the decision about which projects would go and

20   which would stay?

21   A.  So the majority of Josh's projects were meant to remain

22   behind.  There were two projects, I believe, that were to go

23   with him.  If I recall correctly it was Shattered Assurance and

24   another tool.

25   Q.  Did you take over any of Mr. Schulte's projects?

1    A.   I don't believe so.

2    Q.   So what, if anything, did you do after learning of the

3    project reassignments?

4    A.   So when the reassignment happened, I would have went and

5    updated the project permissions so that the proper developers

6    would have had access to the project.

7              MR. LOCKARD:   Thank you, Ms. Cooper.   We can take that

8    down.

9    Q.   Mr. Weber, are you familiar with a project called OSB

10   Libraries?

11   A.   Yes, I am.

12   Q.   And during your time at OSB, what was OSB Libraries?

13   A.   So OSB was frequently responsible for what we referred to

14   as QRCs -- Quick Reaction Capabilities.   Our focus was on

15   tailoring capabilities to mission requirements that often had a

16   very near-term solution, near-term deadline.   The OSB Libraries

17   were conceived as a way of making sure that we were able to,

18   most effectively, be able to meet those deadlines while

19   delivering a capability that was going to be able to meet

20   mission requirements.

21   Q.   And in sort of the Atlassian ecosystem, where did OSB

22   Libraries live?

23   A.   They existed on Stash as a project within Stash.

24   Q.   And who are the original administrators of OSB Libraries?

25   A.   It would have been, if I recall correctly, myself, Josh,

1    Frank, and Matt.

2    Q.  And just to clarify, is that an Atlassian administrator

3    role or project administrator role?

4    A.  Project administrator role.

5    Q.  And what responsibilities did the OSB Libraries project

6    administrators have?

7    A.  So project administrator, in general in Stash, their job

8    was to be able to say who could access a project as well as

9    update -- update work flows and things like that.  For the OSB

10   Library specifically we also had specific permissions assigned

11   that would allow code changes to what is referred to as long

12   live branches.  So in software development this was the known

13   good in a delivered code.  The project administrators would be

14   the ones that did the final -- the final merge of any new

15   changes to that code baseline.

16   Q.  So what, if anything, did you do with Mr. Schulte's

17   privileges to the OSB Libraries project when he moved branches

18   to RDB?

19   A.  Since Josh was no longer in OSB he was removed from the

20   administration of the OSB Libraries.  He was still able to

21   access them and commit to them, but that final ability to merge

22   into the code base would have been removed from him.

23   Q.  Did there come a time when Mr. Schulte spoke to you about

24   the change in his permissions?

25   A.  Yes.

1    Q.  Can you describe that conversation?

2    A.  He came up to me wanting to know what had happened and why

3    it was removed.  He was agitated by it.  I explained to him

4    that since he was no longer in OSB that he wouldn't have that

5    final authority on what could be merged into OSB because we

6    needed to maintain -- we need to maintain integrity of that

7    code base.  He felt that that was a wrong decision and that he

8    would go and talk to Sean about that.

9    Q.  And did you have another conversation with Mr. Schulte

10   after that?

11   A.  Yes.  After Josh went and talked to Sean, he came back to

12   my desk and said that Sean agreed with him and that the

13   permission should be reapplied.  And I told him that I

14   confirmed that with Sean and take the -- you know, do what I am

15   told to do.  Josh then finished it -- I can't remember the

16   exact wording but finished the conversation with telling me

17   that I should go ahead and reapply the permissions now because

18   he would get it back one way or another.

19   Q.  At that time did you believe that you were authorized to

20   give Mr. Schulte permissions back to OSB Libraries?

21   A.  What Josh had explained to me was not what Sean had

22   conveyed to me in the past so this was different and that's why

23   I told Josh that I would confirm that with Sean before I made

24   any changes.

25   Q.  After the second conversation did you speak with anyone?

M6S5sch2                        Weber - Direct

1    A.   Yes.

2    Q.   Who did you speak with?

3    A.   I went and talked to Sean, my branch chief.

4    Q.   During that conversation did Sean tell that you it was OK

5    to make --

6              MR. SCHULTE:  Objection.  Hearsay.

7              THE COURT:  Overruled, but ladies and gentlemen I will

8    permit the witness to answer but you may not consider the

9    statement attributed to Sean for its truth, just for the effect

10   that it had on the witness and what actions, if any he took, as

11   a result.

12             You may answer.

13   A.   Sean -- Sean informed me that that wasn't the case and that

14   things should be left as they are.  He also asked that I send

15   Josh an e-mail explaining exactly what his role should be.

16             MR. LOCKARD:  If we could look at exhibit 1061 and

17   especially page 4 trailing over to page 5.

18   Q.   Mr. Weber, did you send an e-mail that Sean asked you to

19   send?

20   A.   Yes, I did.

21   Q.   Is this that e-mail?

22   A.   Yes, it is.

23   Q.   And who did you send the e-mail to?

24   A.   I sent it to Josh.

25   Q.   And who did you copy?

1    A.   I copied Sean, my branch chief; Anthony, who was the

2    division chief so Sean's boss; Richard, who was the most senior

3    developer within OSB at the time and was going to be eventually

4    stepping in as -- Sean had been selected for a new position and

5    Richard was going to inherit the branch chief responsibilities

6    temporarily; and frank who was one of the major project admins.

7    Q.   So just looking at the first sentence where you say:   I

8    discussed things with Sean and this is the situation.   Had you

9    discussed this with Sean?

10   A.   Yes, I had.

11   Q.   Did you believe this reflected his view?

12   A.   Yes, it does.

13   Q.   And without reading through the entire e-mail, sort of

14   bottom line summary, what did you convey in this e-mail?

15   A.   That the permissions as they were set up were correct and

16   that Josh would no longer be a project admin for the OSB

17   Libraries.

18        MR. LOCKARD:   If we can scroll up to page 4?

19   Q.   Did you receive this reply from Mr. Schulte?

20   A.   Yes, I did.

21   Q.   How long after you sent your e-mail did Mr. Schulte send

22   his reply?

23   A.   It was shortly thereafter.   It looks like nine minutes

24   separated.

25   Q.   So looking at the third paragraph where it says since the

1    OSB Libraries were initially my idea that stemmed from Brutal

2    Kangaroo... do you agree with that statement?

3    A.   No, I do not.

4    Q.   Why not?

5    A.   The OSB Libraries were something that OSB had discussed

6    extensively for probably years at that point and they did not

7    stem from Brutal Kangaroo.  Brutal Kangaroo was simply one of

8    the first tools that would be leveraging them extensively.

9           MR. LOCKARD:  Thank you, Ms. Cooper.

10   Q.   And again, without reading through the entire e-mail, what

11   is the request that Mr. Schulte makes here in this response?

12   A.   That he would be allowed to continue contributions to the

13   library.

14           MR. LOCKARD:  And if we can scroll up one more e-mail

15   in the chain?

16   Q.   Did you receive this response from Anthony?

17   A.   Yes, I did.

18   Q.   And again, what was Anthony's role at this time?

19   A.   Anthony was leading the Applied Engineering Division.

20   Q.   And as with the other e-mails, without reading through the

21   entirety of the text, what did you understand Anthony's

22   response to Mr. Schulte's request to be?

23   A.   From Anthony's e-mail he wanted to set up a discussion

24   about a path forward to take the OSB Libraries from an

25   OSB-focused project to make it an AED-wide resource and he

1    requested that we work with Jojo to set up a meeting to discuss

2    this extensively.

3    Q.   And as the project administrator for OSB Libraries, what

4    was your understanding about what effect this would have on

5    Mr. Schulte's permissions?

6    A.   I saw there was no -- there was no request to change

7    permissions.  Simply, this was a conversation saying that we

8    needed to develop a plan moving forward.

9    Q.   What, if anything, did you do after receiving this e-mail

10   chain?

11   A.   I don't remember why but I ended up looking at the

12   permissions within the OSB Libraries and saw that they were

13   changed.

14   Q.   What do you mean you don't remember why you checked the

15   permissions?

16   A.   I don't know what -- I don't know what spurred me to go and

17   look at it, if it was to confirm that they were properly

18   applied or if I was suspicious of what Josh would do but,

19   regardless, I ended up looking at the permission before I went

20   home that day.

21   Q.   And what did you learn when you checked the permissions?

22   A.   So when I checked the permissions I had seen that Josh had

23   re-granted his access as a project administrator, and also that

24   he had done it after, after reading and replying to my e-mail.

25   Q.   Now, in light of your discussions with Sean and this e-mail

M6S5sch2                     Weber - Direct

1    chain involving Anthony, did Mr. Schulte have authority to do

2    that?

3    A.   I do not believe so, no.

4    Q.   Why was Mr. Schulte able to do it?

5    A.   Because he was --

6            MR. SCHULTE:  Objection.

7            THE COURT:  Overruled.

8    A.   Because he was an Atlassian administrator.

9    Q.   And at this time who were the Atlassian-level

10   administrators?

11   A.   Josh and I were the Atlassian level administrators.  I

12   believe Patrick also still, potentially, was an administrator

13   at that time although he wasn't functioning as one.  And then I

14   believe ISB had a couple people who were Atlassian

15   administrators but weren't -- they weren't actively, like,

16   engaged in the role.

17   Q.   What was your reaction to seeing Mr. Schulte's changes to

18   his permissions to the OSB Libraries project?

19   A.   I felt this was an abuse of the Atlassian permissions that

20   he had and I felt that management needed to be informed of

21   that.

22   Q.   So what did you do next?

23   A.   I believe I immediately went and talked to Sean, possibly

24   Anthony -- I don't remember.  But definitely also ended up

25   sending an e-mail.

1   Q.  And why did you react so quickly?

2   A.  Because --

3            MR. SCHULTE:  Objection.

4            THE COURT:  Overruled.

5   A.  I reacted quickly because I saw this as a security incident

6   which is something that is at the forefront of concern for the

7   CIA.  I felt leadership needed to be known -- leadership needed

8   to be let known that Josh was abusing, in my mind, his

9   privileges.

10           MR. LOCKARD:  Ms. Cooper, could you please pull up

11  Government Exhibit 1061 and go to page 10 of that exhibit?

12  Possibly page 9?  I'm sorry, 1062.

13  Q.  Mr. Weber, you said you sent an e-mail?

14  A.  Correct.

15  Q.  This is that e-mail?

16  A.  Yes, it is.

17  Q.  When did you send it?

18  A.  I sent it April 14th at 4:40 p.m., so shortly after those

19  other e-mails we reviewed.

20  Q.  So your first sentence reads:  We have a situation with the

21  libraries and the Atlassian products in general.

22           So how did the issue with permissions to the OSB

23  Libraries project specifically relate to the Atlassian

24  products, in general?

25  A.  So what Josh had done to re-enable his access required

1    Atlassisan admin privileges to be able to do that, so his

2    demonstration that he was willing to change permissions without

3    authorization for the Stash products, I felt, could easily

4    apply to any of the Atlassian products and that is why I

5    referenced the Atlassian products in general.

6    Q.   Turning to the last sentence where you say:  I can explain

7    the situation further, but this act has shown he believes

8    access controls shouldn't apply to him.

9        Why was that a significant issue for you?

10   A.   As system administrator you have the ability to circumvent

11   a lot of security practices, you can modify settings so that if

12   you -- you can give yourself access to information that isn't

13   necessarily relevant to your mission and that you don't have a

14   need to know have.  So there is a significant level of trust

15   being involved with being system administrator because of this

16   capability and if you can't trust your system administrator

17   they should not be allowed to do their job.

18           MR. LOCKARD:  Ms. Cooper, if we could go to page 9 of

19   this e-mail?

20   Q.   And looking at the e-mail sent on April 15th from Anthony;

21   did you receive this?

22   A.   Yes, I did.

23   Q.   And when did Anthony send this?

24   A.   He sent it April 15th, the next morning, at 7:29 a.m.

25   Q.   And looking at the first two sentences following the three

M6S5sch2                          Weber - Direct

1   questions starting with "my concern here."

2            My concern here is that if Josh wants to use the

3   libraries and no longer has access to them, that's one thing.

4   On the other hand, if he changed his permissions to enable him

5   to administer the libraries, that's another.

6        Which of those two statements described the scenario here?

7   A.   The latter statement, changing his permissions.

8   Q.   So did you respond to Anthony's three questions?

9   A.   Yes, I did.

10            MR. LOCKARD:   And if we could turn to page 6?

11   Q.   So is this the e-mail that you sent?

12   A.   Yes, it is.

13            MR. LOCKARD:   So looking at page 6 and scrolling to

14   page 7, please?   And then to the top of page 8?

15   Q.   Generally speaking, what does that lengthy description

16   apply to?

17   A.   This explains what the OSB Libraries were meant to

18   accomplish.   The work flow that was meant to be followed by

19   anybody contributing to the libraries and, just generally

20   speaking, how permissions were set up.

21   Q.   And why did you provide so much detail about the libraries?

22   A.   Anthony had asked about it in the previous e-mail and I

23   felt more relevant -- he had asked those two questions you

24   referenced, he asked if Josh would have still had the ability

25   to use and contribute to the libraries and this was explaining

1   the way that you were supposed to be able to use and contribute

2   to.

3   Q.  So looking on page 8 and then focusing in on the paragraph

4   numbered 3 here, is this a description of your conversation

5   with Mr. Schulte the previous day?

6   A.  Yes, it is.

7   Q.  And in the second sentence where you say:  I informed him

8   that this was a decision that Sean had made, and that I agreed

9   with the decision; is that a statement that you conveyed to

10  Mr. Schulte the day before?

11  A.  Yes.

12          MR. SCHULTE:  Objection.

13          THE COURT:  Sustained as to form.

14  Q.  What did you tell Mr. Schulte the day before?

15  A.  I had informed him that OSB -- Sean had made decisions

16  about his project, which projects he would retain and that I

17  agreed with that decision.

18          MR. LOCKARD:  Thank you, Ms. Cooper.  We can take that

19  down.  I think we can take down 1062.

20  Q.  Mr. Weber, did you learn of any decisions that were made

21  after you sent that report to Anthony?

22  A.  Yes.

23  Q.  What decision did you learn of?

24  A.  It was decided that this would be -- it was decided that

25  administrative abilities or responsibilities would officially

M6S5sch2                         Weber – Direct

1    transfer from AED to ISB.

2    Q.  You testified earlier that that had been the plan since the

3    beginning; is that right?

4    A.  That was always our intention, correct.

5    Q.  And why was it happening now?

6    A.  I assumed --

7              MR. SCHULTE:  Objection.

8              THE COURT:  Sustained.

9    Q.  Did anyone tell you why it was happening now?

10             MR. SCHULTE:  Objection.

11             THE COURT:  Overruled.

12             Just yes or no.

13   A.  Yes.

14   Q.  And what were you told about why it was happening now?

15             MR. SCHULTE:  Objection.

16             THE COURT:  Sustained.

17   Q.  Who told you why it was happening now?

18             MR. SCHULTE:  Objection.

19             THE COURT:  Overruled.

20   A.  Anthony.

21   Q.  What were the changes that were going to be made to

22   Atlassian privileges?

23             MR. SCHULTE:  Objection.

24             THE COURT:  Overruled.

25   A.  The Atlassian administrative responsibilities would be

1   transferred to ISB, so specifically any AED Atlassian

2   administrators were supposed to be removed from those roles and

3   any user names and passwords used to log into the machines were

4   meant to be updated and replaced.

5   Q.   Now, when you said that AED developers would be removed as

6   administrators, did that include yourself?

7   A.   Yes.

8   Q.   And did it include Mr. Schulte?

9   A.   Yes.

10  Q.   What role did you play in the transfer of privileges?

11  A.    It was requested that I would come in on Saturday with ISB

12  as a means to test that what they -- the changes that they

13  would go forth and implement were accurate.  So essentially I

14  was supposed to be there to answer questions if they had them

15  but at the end of the day I was supposed to try and log in to

16  the Atlassian products and make sure that I wasn't able to

17  access administrative capabilities.

18  Q.   Did you speak with anyone else about the fact that you were

19  coming in on Saturday to do that?

20  A.   No, I didn't.

21  Q.   So what, if anything, did you and the ISB officer do before

22  starting the process of changing the privileges?

23  A.   As I mentioned earlier, good practice for whenever you are

24  making changes to a system was to take a snapshot of the VM so

25  that if you made a mistake you could revert back to it, so we

1    took a snapshot of the Confluence and Bamboo VM.

2    Q.  At the end of that process did you in fact test your

3    permissions?

4    A.  Yes, I did.

5    Q.  What permissions did you test?

6    A.  So there were a few that I tested.  One, I had public

7    private key pair that originally allowed me to log into

8    Confluence and Bamboo.  I tested that to make sure that it no

9    longer worked, which it didn't.  And then also I logged into

10   each of the Atlassian products to see if -- I had mentioned

11   earlier that there was an icon in the upper right-hand corner,

12   that when I logged in I no longer had that icon and thus didn't

13   have the ability to elevate my privileges to administrator.

14          MR. LOCKARD:  Can we pull up Government Exhibit 1251

15   again?

16   Q.  So you talked about accesses to the Atlassian programs.

17   Did you test any permissions with respect to any servers?

18   A.  Yes, I did.

19   Q.  What servers?

20   A.  So again, tested logging into the Stash server, tested

21   logging into the Confluence and Bamboo VMs, and the Jira server

22   as well.

23   Q.  And as a result of that, had your administrator privileges

24   been revoked?

25   A.  Yes.

1    Q.   Were there any changes made to access to the ESXi server

2    that day?

3    A.   Yes.

4    Q.   Who made those?

5    A.   I did.

6    Q.   What did you change?

7    A.   I changed the password on the ESXi server.

8            MR. LOCKARD:   Thank you, Ms. Cooper.   If we could

9    please look at Government Exhibit 1064?

10   Q.   So Mr. Weber, do you recognize this e-mail?

11   A.   Yes, I do.

12   Q.   Did you receive it?

13   A.   Yes, I did.

14   Q.   And who sent it?

15   A.   This was sent by Anthony.

16   Q.   And when was this sent?

17   A.   This would have been sent on the 18th, so I believe that

18   would have been the Monday after, and it was sent at 1:30 in

19   the afternoon.

20   Q.   If we could please focus in on the second paragraph where

21   it states, in the third from the bottom line:   SED/ISB; what is

22   that acronym a reference to?

23   A.   That is division that ISB is part of and ISB is the

24   Infrastructure Branch.

25   Q.   So ISB transferred all system admin responsibilities across

1      all Atlassian products to SED/ISB removing local admin rights

2      from all local AED branch system admins this past weekend.

3           After the events on April 16th and this e-mail from

4      Anthony, did you have any authority to exercise Atlassian

5      administrator privileges?

6      A.   No, I did not.

7      Q.   Did you have any authority to exercise server

8      administrative privileges on the Stash server?

9      A.   No, I did not.

10     Q.   Did you still have authority to exercise administrator

11     privileges on the OSB ESXi server?

12     A.   Yes, I did.

13     Q.   Why is that?

14     A.   The OSB ESXi server was a server that was meant to support

15     OSB's development mission and still remained an OSB

16     responsibility.

17           MR. LOCKARD:   Thank you, Ms. Cooper.   We can take that

18     down.

19     Q.   You described earlier how, when you were an Atlassian

20     administrator, you were able to access the Altabackups folder

21     through the mount point?

22     A.   That's correct.

23     Q.   After April 16th and 18th, did you have authority to access

24     the Altabackups folder?

25     A.   No, I didn't.

M6S5sch2                          Weber - Direct

1    Q.   So after the permissions, the administrator privileges

2    transfer on April 16th, were there any other steps taken with

3    respect to the Atlassian products?

4    A.   Yes, there were.

5    Q.   What else happened?

6    A.   The ISB, in taking over the products, wanted to accomplish

7    two things further.  One was to get all of the products running

8    on ISB-owned and controlled infrastructure so Confluence and

9    Bamboo coming off of OSB infrastructure and moving to ISB

10   infrastructure, as well as there was an intention to update

11   that to run on Windows, again, because they were primarily a

12   Windows development shop.

13           MR. LOCKARD:  Ms. Cooper, can we look at Government

14   Exhibit 1069?

15   Q.   Mr. Weber, do you recognize this e-mail dated April 20th of

16   2016?

17   A.   Yes, I do.

18   Q.   And are you included in those distribution groups?

19   A.   Yes, I am.

20   Q.   And what event does this e-mail relate to?

21   A.   This e-mail is -- Bob, the chief of the Infrastructure

22   Support Branch, letting people know that they would be

23   transferring the Atlassian products to ISB infrastructure and

24   that there would be an outage, potentially.

25   Q.   At this time what Atlassian products were not on ISB

M6S5sch2                    Weber - Direct

1    infrastructure?

2    A.   This would be Confluence and Bamboo.

3    Q.   What, if anything, would have happened to the OSB server

4    during the transfer?

5    A.   Ideally nothing would happen to the OSB server other than

6    resources would eventually be freed up.

7           MR. LOCKARD:  Ms. Cooper, can we take a look at

8    Government Exhibit 1095?  And if we could focus in on the

9    middle of this page, paragraph 1?

10   Q.   So Mr. Weber, I would like to direct your attention to a

11   couple of sentences here within this paragraph, specifically

12   the second sentence where it says:  At the conclusion of the

13   final discussion with Mr. Weber on Thursday, 14th of April

14   2016, Mr. Schulte reportedly remarked that he "will eventually

15   get access back to the libraries and that his access should

16   just be re enabled now" to Mr. Weber before Mr. Schulte left

17   the area.

18        Upon reading the above, Mr. Schulte remarked that his exact

19   quote was that "I am adding my access back, until someone with

20   authority advises me otherwise."

21        Did Mr. Schulte tell you that he was adding his access back

22   until someone with authority advised him otherwise?

23   A.   No, he did not.

24           MR. LOCKARD:  Thank you, Ms. Cooper.  If we can look

25   at Government Exhibit 1081?

1    Q.  So in this e-mail dated June 3rd of 2016, I would like to

2    direct your attention to the fourth paragraph and then starting

3    with the sentence that says:  I notice that he -- referring to

4    Jeremy Weber -- removed my access on April 14th, and I

5    confronted Weber.  He told me that he removed my access because

6    I was no longer in OSB and if I had a problem with it, then I

7    could talk to Sean.  He never once told me he was granted

8    permission from EDG or CCI to remove my access.

9               During your conversation with Mr. Schulte on April

10   14th, had you told him who authorized his removal from OSB

11   Libraries?

12   A.  That topic of conversation did come up.

13   Q.  And then it says:  After discussing with Sean, Sean said he

14   did not give Weber access on April 4th to remove my access.

15       Was that your understanding at the time?

16               MR. SCHULTE:  Objection.

17               THE COURT:  Sustained.

18   Q.  Let's move to the next paragraph.  Directing your attention

19   to the sentence:  Jeremy Weber took advantage of the situation

20   of me moving branches due to a security incident of another

21   employee threatening to kill me, and took over all my projects.

22       Mr. Weber, when Mr. Schulte transferred to RDB, did you

23   take over any of his projects?

24   A.  I don't believe so.

25   Q.  Then the next sentence:  He specifically told me that he

1    did not like how I disagreed with him on my project so he took

2    advantage knowing no one would punish him to take over all of

3    my projects.

4         Do you agree with that statement?

5    A.   No, I don't.

6    Q.   Why not?

7    A.   I often actually -- I often engaged with Josh because I

8    like the robust conversation that we had about the direction a

9    project should go, I felt that it was always fruitful.  I did

10   not take advantage of the situation with an intent to punish

11   him.  My actions were based on ensuring that OSB would be able

12   to continue to meet its mission and the people who had been

13   assigned the projects were able to work on them.

14             MR. LOCKARD:  Thank you, Ms. Cooper.  Can we please

15   look at Government Exhibit 1093?

16   Q.   So in this June 28, 2016 e-mail from Mr. Schulte, if I can

17   please direct your attention to the second page and then the

18   top paragraph?  Directing your attention to the sentence that

19   begins:  One day I found that my access to the OSB Libraries, a

20   library of code that I had created and was responsible for

21   maintaining, had oddly revoked my access.  Strange, but not

22   abnormal -- there were constant issues with the software where

23   people's accesses were removed or projects left without

24   permissions, which I had dealt with for years.

25        During your time as an Atlassian administrator, were you

1    aware with situations where projects were left without

2    permissions?

3    A.  Yes.

4    Q.  Are you familiar with situations where people's permissions

5    were revoked for no reason?

6    A.  No.

7    Q.  Directing your attention to the next sentence:  So

8    naturally, I simply added my accesses back to my projects.  I

9    then looked at the audit logs and found that the only other

10   Stash administrator -- Jeremy Weber -- had been the one to

11   remove my access.  I spoke with him and he told me that since I

12   had moved branches I was no longer in charge of the project.

13        Did Mr. Schulte change his permissions before or after he

14   spoke with you?

15   A.  After he spoke with me.

16           MR. LOCKARD:  Thank you, Ms. Cooper.  Ms. Cooper,

17   could we please show Mr. Weber what's been marked for

18   identification Government Exhibit 806?  And if you could turn

19   to page 2?

20   Q.  Mr. Weber, do you recognize the handwriting on this page?

21   A.  Yes, I do.

22   Q.  Whose handwriting is it?

23   A.  Joshua Schulte's.

24           MR. SCHULTE:  Objection.  It is not in evidence.

25           THE COURT:  Overruled.

M6S5sch2                         Weber - Direct

1            MR. LOCKARD:  The government offers 806.

2            THE COURT:  Any objection?

3            MR. SCHULTE:  Yes, we object coming through this

4    witness.

5            THE COURT:  Overruled.  Admitted.

6            (Government's Exhibit 806 received in evidence)

7            MR. LOCKARD:  So, Ms. Cooper, if we could please

8    expand the text portion of this page?

9    Q.  Mr. Weber, can you help decode this for us?

10   A.  Do you want me to read it?

11           MR. SCHULTE:  Objection.

12   Q.  If you can please read what is written here?

13   A.  Small files are retained in file record whereas large files

14   are stored in Microsoft's -- I'm not sure what that word is.

15   If you need help, ask WikiLeaks for my code.  I developed

16   sufficient parsers -- MSFT is -- sorry, MSTF is an abbreviation

17   for Microsoft -- NTFS and EXT 3 partitions so that I --

18   blank -- for a operation.

19   Q.  You mentioned that MSFT stands for Microsoft?

20   A.  Yes.

21   Q.  And what is NTFS?

22   A.  NTFS is a file system primarily used in the windows

23   operating system.  It stands for NT File System.  Windows NT

24   was a product of Microsoft's.

25   Q.  And what is EXT 3 partitions?

1    A.  EXT 3 was a different file system, primarily used in Linux

2    operating systems.

3    Q.  Generally speaking, what do these statements relate to?

4           MR. SCHULTE:  Objection.

5           THE COURT:  I will allow you to state your

6    understanding just generally what they relate to.

7    A.  So, working -- collecting files sometimes involves direct

8    interaction with file systems to be able to collect those

9    files.  These parsers were code Josh claims to have written to

10   enable that.

11   Q.  And what effect would it have on the CIA's cyber mission to

12   disclose this type of mission about a particular operation?

13          MR. SCHULTE:  Objection.

14          THE COURT:  Overruled.

15   A.  The concern would be surrounding attribution.  The more

16   hints and evidence that you give to the security community, the

17   better posed they are to be able to detect your capabilities as

18   well as potentially attribute it to a certain actor's activity.

19   Q.  How, if at all, would that risk be affected by directing

20   readers to a place like WikiLeaks which is claimed to have the

21   source code?

22          MR. SCHULTE:  Objection.

23          THE COURT:  Sustained as to form.

24   Q.  How, if at all, would linking the techniques described here

25   for a particular operation to published source code affect

1    those risks?

2              MR. SCHULTE:  Objection.

3              THE COURT:  Overruled.

4    A.   The concern would be, again, making a statement that the

5    source code that was in the public was source code that was

6    written by the CIA and, thus, any tool compiled with that

7    source code is a CIA tool.

8    Q.   And again, focusing on the identification of an operation,

9    what types of risks would that pose to people involved in the

10   operation?

11             MR. SCHULTE:  Objection.

12             THE COURT:  Sustained.  Asked and answered.

13             MR. LOCKARD:  If we could turn to Government Exhibit

14   809 and just for Mr. Weber?  And if we could turn to page 2 of

15   809?

16   Q.   Mr. Weber, do you recognize this handwriting?

17   A.   Yes, I do.

18   Q.   Whose handwriting is it?

19   A.   Joshua Schulte's.

20             MR. LOCKARD:  The government offers Exhibit 809.

21             THE COURT:  Any objection?

22             MR. SCHULTE:  Same objection.

23             THE COURT:  Same ruling; admitted.

24             (Government's Exhibit 809 received in evidence)

25             THE COURT:  And let me make clear, these admissions

1    are subject to connection.

2              Go ahead.

3              MR. LOCKARD:  Thank you, your Honor.

4              Can we please publish 809 and if we could focus in on

5    the block of text in the upper right-hand sort of third?  I

6    guess all of the text is what I was inartfully trying to

7    describe.

8    Q.  So Mr. Weber, could you please read the handwritten

9    statements that begin with the word "if" in the top middle?

10   A.  If -- I'm not sure what that second word is -- doesn't pay

11   me $50 billion in restitution and prosecute the criminals who

12   lied to the judge and presented the BS case, then I will visit

13   every country in the world and bear witness to the treachery

14   that is the U.S.G.  I will look to break up diplomatic

15   relationships, close embassies, and U.S. -- something -- across

16   the world and finally reverse U.S. -- I'm not sure what that

17   word is.  If this is the way the U.S. -- oh, I think that's

18   U.S. G-O-V-T for government -- treats one of their own --

19   something -- do you think they treat allies.

20              (Continued on next page)

21

22

23

24

25

M6sWsch3                          Weber - Direct

1              THE COURT:  Ladies and gentlemen, just to be clear, in

2      part, just so you can understand and appreciate the exhibit,

3      given Mr. Weber's familiarity with Mr. Schulte's handwriting,

4      I'm permitting him to read it.  But ultimately, what weight, if

5      any, you put on these exhibits and how you read them is your

6      decisions to make.

7              You may proceed.

8              MR. LOCKARD:  Thank you, your Honor.

9      Q.  What, if any, relationship is there between foreign

10     relations and disclosure of information about the CIA?

11             MR. SCHULTE:  Objection.

12             THE COURT:  Overruled.

13     A.  The -- again, the CIA is meant to operate in secret, and so

14     publicly -- publicly outing CIA operations, the concern about

15     diplomatic relationships is always at the forefront.

16             MR. LOCKARD:  If we could turn to page 8 of this

17     exhibit.

18     Q.  And again, do you recognize this handwriting?

19     A.  Yes, I do.

20     Q.  Whose handwriting is this?

21     A.  Josh Schulte's.

22     Q.  If we could focus in on the bottom third or fourth of this

23     page.

24         Mr. Weber, could you please read the part that starts with

25     the text in the black box, "tool from vendor report"?

1   A.   Read from that point on?

2   Q.   Yes, just through the end of that line.

3   A.   "Tool from vendor report, Bartender for vendor."

4   Q.   And then I think also if we can turn on page 10, focusing

5   in on the top quarter or so of that page.

6        If you could please read the portion in the box that says

7   "just to authenticate me first"?

8   A.   Yeah.  "Just to authenticate me first, the @CIA was

9   involved in," and it's blacked out.  "The code for initially

10  planned cyber operations is in Vault 7.  Additionally, tool

11  described in vendor report is, in fact, Bartender.  CIA tool

12  set for operators to configure for deployment."

13  Q.   Mr. Weber, are you familiar with something called

14  Bartender?

15  A.   Yes.

16  Q.   And without any specifics, what was Bartender?

17  A.   Bartender was a project I was primarily responsible for

18  that was capabilities that we gave for the human-enabled

19  operations.

20  Q.   Did Mr. Schulte play any role in Bartender?

21  A.   Yes.

22  Q.   And why was that?

23  A.   I requested he join my team.  I felt that he would be a

24  value added for the development of the tool.

25  Q.   Did there come a time when Bartender was described in a

1  vendor report?

2  A.  Yes.

3  Q.  Without getting into any details, did that vendor report

4  identify Bartender as a CIA tool?

5  A.  No, it did not.

6  Q.  What, if any, concerns did you have about the fact that

7  Bartender had been described in a vendor report?

8  A.  The concern we had at the time was that other vendors would

9  be able to leverage this to become increasingly good at

10  catching the deployment of this tool.  So in a sense, when the

11  vendor report came out, we made a decision that we would have

12  to significantly reengineer it to continue its use.

13          THE COURT:  Could you just explain what you mean by a

14  vendor report?

15          THE WITNESS:  A vendor report, somebody in the

16  security community -- an antivirus vendor specifically -- had,

17  did a detailed description of a portion of the tool that was

18  caught in the wild.  These vendor reports are somewhat common.

19  Vendors, when they catch something that's interesting, will

20  write up about it so that in, like, the greater community can

21  know about it.

22          THE COURT:  That was a public report, not within the

23  CIA?

24          THE WITNESS:  This was a public report, correct.

25  BY MR. LOCKARD:

1    Q.   And did the vendor report, was it completely accurate about

2    the tool?

3    A.   No, it was not.

4    Q.   Now, Mr. Weber, was information about Bartender disclosed

5    by WikiLeaks?

6    A.   Yes.

7    Q.   So if information about Bartender was publicly disclosed by

8    WikiLeaks and if this vendor report was also publicly

9    available, what, if any, harm could be caused by linking the

10   two?

11            MR. SCHULTE:   Objection.

12            THE COURT:   Overruled.

13   A.   The concern with the WikiLeaks thing, the WikiLeaks

14   disclosure was on the side of the attribution side of it.   The

15   tool -- the tool -- the vendor report made no attribution

16   claims about which, which actor used the capability or how it

17   was used.   The disclosures in WikiLeaks both gave insight into

18   the intentions of the tool, how -- how witting the asset was to

19   deploying it, as well as, again, tying that tool to the CIA and

20   thus tying the asset to the CIA.

21   Q.   And again, without getting into any specifics, what are the

22   attribution concerns with a human-enabled operation?

23   A.   So, for a human-enabled operation the concern is tying,

24   tying a human to the CIA, labeling him as a CIA spy, and the

25   retribution that could occur to them.

1    Q.   I think you said that Mr. Schulte had worked on the

2    Bartender tool?

3    A.   Yes.

4              MR. SCHULTE:  Objection.

5    Q.   Had you discussed with Mr. Schulte attribution concerns

6    like you've described today?

7    A.   Yes.

8    Q.   How often was that a topic of conversation?

9    A.   In general, it was a frequent topic of conversation.  It

10   was always -- within developing in AED, there's never enough

11   time, there's never enough resources to do things perfectly.

12   So different risks have to be weighed against each other.  And

13   one of the biggest risks that we always concern ourselves with

14   is attribution and any risks that development decisions might

15   put on kind of the attribution scale, specifically for

16   Bartender, because the focus of the class of assets that would

17   use the tool, attribution was the greatest concern that we had

18   for any development decisions we made.

19             THE COURT:  Can I just clarify.  When you say

20   attribution concern, is the concern that once a program source

21   code is in the world and available, that somebody could look at

22   it, that's one thing, but to look at it and then know that it

23   came from the CIA is another thing; is that what you mean by

24   attribution?

25             THE WITNESS:  Yes.  If I could expand on it a little

1   bit?

2              THE COURT:  Yes.  Just do it into the microphone.

3              THE WITNESS:  Sorry.

4              So, in terms of attribution, one of the big concerns

5   often is linking two tools together.  So a tool is deployed in

6   one location of the world and then a separate tool is deployed

7   in another location.  Generally speaking, in terms of CNE,

8   there are different ways of linking -- linking activity

9   together.  You'll see this all the time, if you follow

10  reporting on APT groups in the public, of essentially antivirus

11  vendors and security researchers trying to make assumptions

12  about something new that was discovered based on something that

13  they've seen before.

14             So if -- if tool a is captured in the wild and the

15  vendor, for various reasons, makes a decision that they feel

16  that this is tied to a certain actor, and they -- another tool

17  is captured, they'll look at that and see what tradecraft

18  decisions, possibly what code reuse decisions are made, to try

19  and link the tools in it together so that they could have a

20  justification for why something else is attributed.  So having,

21  again, publicly -- publicly disclosed statements verifying that

22  an attribution -- something is attributed to someone helps

23  bolster the claims of secondary attribution.

24             I hope that answers your question.

25             THE COURT:  I think so.  But further clarification,

M6sWsch3                        Weber - Direct

1       when you say captured in the wild, I take it you mean just out

2       in the public domain when source code is identified; is that

3       what you mean?

4                  THE WITNESS:  So, often what I refer to as captured in

5       the wild, I'm sure most of us have either encountered antivirus

6       products or run antivirus on your home computer.  When you get

7       a pop-up saying that a virus has been found on your computer,

8       that, in my terms, is being caught in the wild.  I'm not

9       saying, obviously, that what popped up on your computers would

10      be us, but -- so oftentimes, when it comes to CNE, captured in

11      the wild means a tool was attempted to be deployed, but

12      defensive countermeasures caught it, and often security

13      communities will send that to a security researcher to tear it

14      apart, so to speak.  They will do a full review of it to see

15      what it's doing, how it's doing it, to see THAT if there's

16      anything that should be updated so computers can be safer

17      worldwide.

18                 THE COURT:  Last question for the moment.  You said

19      CNE a couple times.

20                 THE WITNESS:  I apologize.  You live this long, the

21      lingo --

22                 CNE stands for computer network exploitation.

23      Generally speaking, we use it as a broad term covering

24      everything involved with hacking activity.

25                 THE COURT:  All right.  You may proceed, Mr. Lockard.

M6sWsch3                          Weber - Direct

1              MR. LOCKARD:  Thank you, your Honor.

2                   If I could have just one moment, your Honor?

3                   Could we turn to just the next page of this exhibit.

4    Q.  Mr. Weber, do you recognize the handwriting on this page?

5    A.  Yes, I do.

6    Q.  And whose handwriting is it?

7    A.  Joshua Schulte's.

8    Q.  In the upper right-hand corner --

9              MR. LOCKARD:  Ms. Cooper, if we could please expand

10   that.

11   Q.  -- can you read what's written here?

12   A.  Yes.  "#top secret.  #fuck your top secret.  Attempted or

13   dump the secrets here."

14             MR. LOCKARD:  Thank you.

15             Ms. Cooper, if we could zoom back out, and if we can

16   zoom in on sort of the third fifth of that page, where it

17   starts "@vendor."

18   Q.  OK.  Mr. Weber, does this statement relate to what we've

19   just been talking about?

20   A.  Yes, it does.

21   Q.  Describing the same Bartender tool suite?

22             MR. SCHULTE:  Objection.

23             THE COURT:  Overruled.

24   A.  Yes, it does.

25   Q.  And what is the last line of this particular statement,

M6sWsch3                       Weber - Direct

1    starting with "this source code"?

2    A.   "This source code is available in the Vault 7 release."

3              THE COURT:  Ladies and gentlemen, this is a good

4    moment for me to just remind you that I've approved various

5    redactions in some of the exhibits that are in evidence -- not

6    just redactions but some substitutions, as I told you a week or

7    so ago.  Just a reminder that you shouldn't speculate as to the

8    reasons for that or as to what is behind the redactions.  It's

9    only the portions that are unredacted that you should concern

10   yourselves with.

11             Thank you.

12             MR. LOCKARD:  No further questions, your Honor.

13             THE COURT:  All right.

14             Cross-examination.

15             JUROR:  Your Honor?

16             MR. LOCKARD:  I think we have a question, your Honor.

17             JUROR:  Could I use the bathroom?

18             THE COURT:  Sure.  While we're switching,

19   Ms. Smallman, if you could take juror No. 13 to the restroom.

20             If the rest of you want to stretch where you are,

21   you're welcome to.  Obviously we're taking our break in not too

22   long.

23             Juror No. 13, if you could put your mask back on,

24   please.

25             Thank you.

M6sWsch3                         Weber - Cross

1              All right.  You can be seated if you were standing.

2              Mr. Schulte, you may proceed with the

3     cross-examination.

4     CROSS-EXAMINATION

5     BY MR. SCHULTE:

6     Q.   Good morning.

7     A.   Good morning.

8     Q.   Mr. Weber, in 2015, you'd been at the CIA for about five

9     years, is that correct?

10    A.   That's correct.

11    Q.   We both started about the same time, right?

12    A.   That's correct.

13    Q.   What was your official title?

14    A.   Software developer.

15    Q.   And I was also a developer, correct?

16    A.   Correct.

17    Q.   We worked in the same branch at that time, right?

18    A.   I believe that's correct, yes.

19    Q.   We were not only colleagues during our time at the CIA, but

20    we were friends outside of work, right?

21    A.   I would say yes.

22    Q.   We played Xbox together, right?

23    A.   Yes.

24    Q.   You introduced me into a game called Dark Souls, right?

25    A.   Yes.

1    Q.   We went skiing together, right?

2    A.   That's correct as well.

3    Q.   Went to several outside events together, right?

4    A.   Yes.

5    Q.   Sometimes watched hockey together, right?

6    A.   Tried to get you into hockey.

7    Q.   I even housesat for you when your new furniture came in,

8    right?

9    A.   That's correct too.

10   Q.   We spoke of personal matters, correct?

11   A.   Yes.

12   Q.   You considered me patriotic, correct?

13   A.   Yes.

14   Q.   Supportive of the mission at the CIA, right?

15   A.   Yes.

16   Q.   You observed that I loved my work, right?

17   A.   I think so, yes.

18   Q.   And that I especially enjoyed working on counterterrorism

19   operations, correct?

20   A.   I don't know -- I don't know if you ever demonstrated a

21   distinction between which ops you liked working on.

22   Q.   OK.  Over the time we worked together, I never talked about

23   WikiLeaks, right?

24   A.   No.  You did.

25   Q.   OK.  What was the discussion on WikiLeaks?

1    A.   You often referenced WikiLeaks and more specifically, if I

2    recall, Julian Assange, and often, often spoke of wanting to

3    see them executed.

4    Q.   OK.   And you considered me a person who had strong

5    opinions, correct?

6    A.   I think that's a fair statement.

7    Q.   You knew that I was critical of Manning and Snowden's

8    leaks, correct?

9    A.   Yeah, I believe so, yes.

10   Q.   And as you already said, I thought that leakers should be

11   executed, right?

12   A.   Yes, I do remember you saying that on more than one

13   occasion.

14   Q.   And my opinions on this topic were public, correct?

15   A.   It was something that you said out in the open, at least in

16   the vault.

17            THE COURT:   Can you just explain Manning and Snowden,

18   just in case folks don't know who those people are; can you

19   just explain who they are?

20            THE WITNESS:   Yes.   So, in reference to this, I assume

21   Manning being at the time Bradley Manning, now Chelsea Manning,

22   who was a leaker.   I don't know if they were in conjunction

23   with WikiLeaks, but they have been -- she is spending or at

24   least spent time in prison.

25            And then Snowden being Edward Snowden, the accused NSA

M6sWsch3                        Weber - Cross

1    leaker.

2    BY MR. SCHULTE:

3    Q.  And the time frame of these topics of conversation?

4    A.  I assume certain of the time they happened.  I don't

5    remember the times that those leaks occurred.

6    Q.  OK.  It was clear to you that I strongly believed in the

7    mission of the CIA, correct?

8    A.  You -- you stated as such.

9    Q.  And I strongly believed that you should not do anything

10   against America, correct?

11   A.  I -- I wouldn't -- I wouldn't see you saying something

12   otherwise.  I don't know if I ever heard you say that

13   specifically.

14   Q.  OK.  After the leak, you were interviewed by the FBI,

15   correct?

16   A.  Yes.

17   Q.  Stash was stolen, correct?

18   A.  Portions of Stash have been demonstrated to be in the

19   leaks.

20   Q.  OK.  But Stash contained many tools that I worked on,

21   correct?

22   A.  Yes, it did.

23   Q.  A lot of my own work was compromised, correct?

24   A.  I don't -- I don't recall the exact list of what was, what

25   was outed from Stash.

M6sWsch3                          Weber - Cross

1   Q.   OK.  But you testified on direct that you basically had to

2   start over your work, right?

3   A.   We did.

4   Q.   OK.  So all the countless hours or years that I put into

5   that work was gone too, right?

6   A.   Correct.

7   Q.   OK.  Let's talk a little bit about WikiLeaks's publication.

8   As you said, after the WikiLeaks disclosure on March 7, DevLAN

9   was shut down, correct?

10  A.   That's correct.

11  Q.   It was no longer used, right?

12  A.   To my knowledge, correct.

13  Q.   And the tools exposed by WikiLeaks were no longer used,

14  correct?

15  A.   At the time that is correct.

16  Q.   The CIA tool Bartender was shut down, right?

17  A.   The development for it was shut down, correct.

18  Q.   I think as you testified earlier, it was previously -- it

19  was a tool that had been previously exposed, before WikiLeaks,

20  right?

21  A.   Correct.

22  Q.   And I'm not sure how much you touched on this before, but

23  you were part of the recovery effort after the leak, right?

24  A.   I was a portion of -- I don't know if recovery effort is

25  the correct terminology, but making assessments about the leak

M6sWsch3                         Weber - Cross

1    is correct.

2    Q.   Right.  How soon thereafter did you realize the disclosure

3    was from DevLAN?

4    A.   I made an assumption that it was from DevLAN immediately

5    upon seeing -- seeing the printout that was put in front of me

6    the day I arrived.

7    Q.   At that time you had no idea when the data was taken,

8    correct?

9    A.   That is correct.

10   Q.   Hickok was shut down too, correct?

11            MR. LOCKARD:  Objection.

12            THE COURT:  Sustained.

13   BY MR. SCHULTE:

14   Q.   Was Hickok shut down?

15            MR. LOCKARD:  Objection.

16            THE COURT:  Sustained.

17            (Defendant conferred with standby counsel)

18   BY MR. SCHULTE:

19   Q.   You wanted to know what was going on in DevLAN, right?

20   A.   I didn't particularly care what was going on in DevLAN.

21   Q.   Well, I mean the networks that were connected to DevLAN.

22   Right?

23   A.   It was not something that I was considering at the time.

24   Q.   But the shutdown of DevLAN had of effect of other networks

25   too, right?

M6sWsch3                        Weber - Cross

1          MR. LOCKARD:  Objection.

2          THE COURT:  Sustained.

3   BY MR. SCHULTE:

4   Q.  It is standard operating procedure to completely close shop

5   after a leak, right?

6          MR. LOCKARD:  Objection.

7          THE COURT:  Let's move on to a different line, and

8   we'll discuss it at the break.

9          Go ahead.

10  BY MR. SCHULTE:

11  Q.  OK.  So you were conducting damage assessment, right?

12  A.  We were -- my team was specifically focused on identifying

13  what was in the leaks and helping -- helping identify what we

14  knew to be out there.

15  Q.  And how many people were on your team?

16  A.  I don't remember the exact number.  Probably about ten,

17  give or take a few individuals.

18  Q.  OK.  This team, was it the WikiLeaks task force?

19  A.  No.

20  Q.  Were you aware of the existence of the WikiLeaks task

21  force?

22  A.  Yes, I was.

23  Q.  Were any CIA assets harmed as a result of the leak?

24          MR. LOCKARD:  Objection.

25          THE COURT:  If you know the answer to that.

M6sWsch3                        Weber - Cross

1    A.   I do not know the answer to that.

2    Q.   You were also aware that the advanced forensic division was

3    also conducting its own investigation, correct?

4    A.   I don't know what exactly they were doing except that

5    they -- they were doing something.

6    Q.   Well, you coordinated with AFD, correct?

7              MR. LOCKARD:  Objection.

8              THE COURT:  Overruled.

9    A.   AFD, there was some limited coordination.  Specifically --

10   the most specific thing was it was requested that I review, I

11   review all of the commit messages in Stash.

12        A commit message, when you change code, a commit is

13   something, a commit message is something that you're supposed

14   to supply to say why you're making the change, so if somebody's

15   reviewing it, they have an idea.  It was requested that I

16   review the commit messages to see if there was anything

17   politically sensitive or embarrassing in there, since it was a

18   free-form thing.  Essentially, they asked me to look to see if

19   there were swears and things like that.

20        AFD specifically created a spreadsheet for me that had that

21   information in it.

22   Q.   And you were aware of the analyses conducted by AFD,

23   correct?

24             MR. LOCKARD:  Objection.

25             THE COURT:  Sustained.

M6sWsch3                     Weber - Cross

1    BY MR. SCHULTE:

2    Q.   Were there many forensic reports filed by AFD about the

3    leak?

4    A.   Not that I'm aware of.

5    Q.   OK.   But at some point you learned that AFD determined the

6    backups from the Altabackups must have been stolen, correct?

7              MR. LOCKARD:   Objection.

8              THE COURT:   Sustained.

9              (Defendant conferred with standby counsel)

10   BY MR. SCHULTE:

11   Q.   You reviewed the AFD reports, correct?

12             MR. LOCKARD:   Objection.

13             THE COURT:   Sustained.

14             Let's move on, Mr. Schulte.

15             (Defendant conferred with standby counsel)

16             THE COURT:   And please keep your voice down when

17   conferring with standby counsel.

18             MR. SCHULTE:   I'm just going to show the witness

19   what's marked as 3507-516.

20             MR. LOCKARD:   Objection.

21             THE COURT:   Hold on.

22             Sustained.

23   BY MR. SCHULTE:

24   Q.   What about the WikiLeaks task force; did they file many

25   reports?

M6sWsch3                          Weber - Cross

1    A.   I'm not sure what the output was of the WikiLeaks task

2    force.

3    Q.   You don't know what their final conclusion was?

4    A.   No, I'm not.

5    Q.   OK.   Sitting here today, you have no idea how much data was

6    stolen, correct?

7    A.   I am not aware of what the final determination was.

8    Q.   OK.   But you are aware that the assessment is that both

9    Stash and Confluence were leaked, correct?

10             MR. LOCKARD:   Objection.

11             THE COURT:   Sustained.

12   BY MR. SCHULTE:

13   Q.   From your analysis after the leak, you were able to

14   determine that both Stash and Confluence were released by

15   WikiLeaks, correct?

16   A.   From what I have seen, information that was in Confluence

17   and information that was in Stash was published by WikiLeaks.

18   Q.   OK.   And from that you can infer that both Stash and

19   Confluence were taken, correct?

20             MR. LOCKARD:   Objection.

21             THE COURT:   Overruled.

22   A.   I -- I didn't -- I don't have an opinion on how this

23   occurred.

24             THE COURT:   Well, let me ask you, given your

25   familiarity with the network, is there a way in which

M6sWsch3

1      information from Confluence and information from Stash would be

2      published on WikiLeaks that wouldn't involve access to both of

3      those?

4            THE WITNESS:  You would have to, based on what I've

5      seen, you would either have to have removed -- removed

6      information directly from Confluence or Stash or accessed the

7      backups in some capacity.

8      BY MR. SCHULTE:

9      Q.   OK.  And both Stash and Confluence relied upon version

10     control, correct?

11     A.    That is correct.  I'm -- Confluence had a version

12     controlling in it, and Stash -- Stash was meant to display

13     Git's version control, which Git is the source control

14     technology that we were using.

15           THE COURT:  All right.  That's where we will stop for

16     our break.

17           Ladies and gentlemen, you know the drill.  Don't

18     discuss the case with one another or anyone else.  Keep an open

19     mind.  Don't do any research about the case.  Please be ready

20     to go at 12:15 so that we can start, hopefully, promptly at

21     12:20.  And with that, enjoy your breaks.

22           Thank you.

23           (Continued on next page)

24

25

M6sWsch3

1           THE COURT:  You may be seated.

2           Mr. Weber, you're welcome to put on your mask and step

3   down.  Please be back in the witness room by 12:15.

4           You are now on cross-examination, which means you

5   should not communicate with anyone from the government

6   regarding the substance of your testimony.  I know there are

7   security-related issues, and obviously you can discuss that

8   with folks, but not the substance of your testimony.

9           THE WITNESS:  OK.  So just to make sure, I'm OK eating

10  lunch in the room?

11          THE COURT:  I actually have no idea where you're

12  allowed to go, but someone back there will tell you.

13          THE WITNESS:  OK.

14          THE COURT:  All I can tell you is get off the stand.

15          All right.  With that, just quickly, so that I give

16  you your breaks, or most of them, first of all, I don't expect

17  any further -- I'll wait until the witness is out of the room.

18          (Witness not present)

19          THE COURT:  I don't expect any further questions about

20  AFD.  I think we've come close to the line as it is, but given

21  the witness's lack of involvement or familiarity with it, I

22  don't expect to see any more questions given that I don't

23  expect that he would have any admissible testimony on it in any

24  event.

25          Anything we need to discuss?  There was a line of

1        questioning, and I'm not remembering what it was, but I said

2        we'd circle back to it at the break.

3                MR. SCHULTE:  Yeah.  It was about the standard

4        operating procedure to close shop.

5                THE COURT:  Right.

6                MR. SCHULTE:  These types of questions are all

7        important.  I'm not sure what the government's issue is.

8                THE COURT:  Mr. Lockard, if we can discuss it in this

9        setting --

10               MR. LOCKARD:  So, I don't think it is important.  I

11       don't think the defendant has explained why it's important, and

12       it certainly implicates things about what the agency's standard

13       response to security breaches is.  And what the agency's

14       standard response to, you know, various items is not pertinent

15       to the issues in this trial.

16               THE COURT:  All right.

17               Mr. Schulte, to the extent that you can in this

18       setting, explain why you think it's not just important but

19       relevant, can you explain?  That was my concern.

20               MR. SCHULTE:  So, the importance and the relevance is

21       the standard operating procedure's not -- it goes to what the

22       knowledge is about what happens when, after a leak -- knowledge

23       that he would know, standard operating procedure; knowledge

24       that I would know, which would mean, you know, that I would

25       know that these tools or this network's being shut down is not

1    being used anymore.  That's the critical point there.  And for

2    Hickok and the other networks too, it's going to the same

3    point.  The fact that these were shut down, and then I, even

4    though I'm not even at the agency, would know that these are

5    being shut down and not being used anymore is relevant for the

6    defense.

7            THE COURT:  But why?

8            MR. SCHULTE:  Well, for the MCC counts.  By the time

9    2018 rolls around, I already know, after 2017, that this

10   stuff's been shut down because it's standard operating

11   procedure and this stuff's not being used anymore.  That's the

12   relevance.  I think he also testified as to damage.

13           THE COURT:  I don't think the government suggested

14   that anything beyond DevLAN was shut down and in that sense

15   it's not, I think, directly relevant to the damage that the

16   government has elicited.

17           Mr. Lockard, I think Mr. Schulte's points about the

18   MCC counts are somewhat well-taken in the sense that the

19   government is proceeding on the theory that certain of his

20   disclosures regarding Hickok were NDI, and in that regard the

21   fact that Hickok was or wasn't -- well, if Hickok was shut down

22   and if Mr. Schulte would've have known that, it may well have a

23   bearing both on whether it's NDI and also whether it was a

24   willful disclosure.

25           MR. LOCKARD:  I think there are two problems.  I think

M6sWsch3

1          the first one is that Mr. Schulte is trying to elicit his

2          knowledge from another witness, and I just don't think he can

3          do that.  I don't think there's a foundation for it, and if

4          Mr. Schulte wants to establish his knowledge, he's got to

5          establish his knowledge.

6                    I think, secondly, as far as the harm issues go, I

7          don't think there's really a dispute in this trial about the

8          fact that the harm and Mr. Schulte's argument that he believes

9          tools were shut down or that he believed the network was shut

10         down doesn't go anywhere near to addressing the types of harms

11         that the witnesses have testified about in this courtroom.

12                    THE COURT:  I'm not concerned about the harms.  I'm

13         concerned about the particular information that Mr. Schulte is

14         accused of leaking or attempting to leak in connection with the

15         MCC charges and its relationship to Hickok.  I think you're

16         probably right that he can't elicit his state of mind or his

17         knowledge through this witness, but I suppose to the extent

18         that it would be absolutely standard operating procedure to

19         take down any network implicated in this, including Hickok, and

20         he can elicit through this witness that that would be known to

21         anyone who was a developer at the CIA and then make an argument

22         for the jury to infer that he would have known that, that may

23         be fair game.

24                    What's your response to that?

25                    MR. LOCKARD:  I think there's another wrinkle in that

1      argument, which is that Mr. Schulte's claim has not been that I

2      didn't think that there was harm.  It has been I didn't think

3      that it was closely held because it was publicly disclosed,

4      which is a completely separate issue than what he's trying to

5      raise now.

6                  MR. SCHULTE:  This is all ridiculous.  I don't think

7      the prosecution can say what the defense theory is, so -- and

8      the point is --

9                  THE COURT:  Well --

10                 MR. SCHULTE:  It is standard procedure to --

11                 (Defendant conferred with standby counsel)

12                 MR. SCHULTE:  And to the degree that the government

13     thinks a certain theory was asserted, the defense has the

14     ability to change whatever defense theory it wants through the

15     trial.  But the point is if this is standard operating

16     procedure and these things are shut down, then there can't

17     be -- it goes to the willfulness.  It goes to many elements of

18     the MCC counts.

19                 MR. LOCKARD:  So, again, there has been extensive CIPA

20     litigation, so it is not the case that the defendant can change

21     his theory on a dime.  But I think more importantly, this

22     witness has testified he does not know what happened.  So to

23     try and speculate about what Mr. Schulte knew based on what

24     standard operating procedure might be, I think, is just not --

25     there's no evidentiary basis for that.

1          MR. SCHULTE:  Well, he wasn't allowed to answer the

2     question because of the objection.  He never said that there

3     wasn't standard operating procedure or that Hickok wasn't shut

4     down or that he didn't have knowledge of that.

5          THE COURT:  All right.  Anyone want to say anything

6     else?  I think otherwise I'll reserve judgment.  I want to look

7     back at the transcript and also think about it over the break,

8     and I'll tell you at the end of the break.

9          MR. SCHULTE:  I just had the one last thing on AFD.

10          The recent 3500 material is where he states certain

11     facts about AFD, and he stated in his testimony that he did

12     facilitate some work with AFD.  So I think that those are --

13     you know, the question specifically about the determinations

14     made by AFD that he is familiar with, I think he has the

15     knowledge to testify about those.

16          THE COURT:  What's the relevance of it?

17          MR. SCHULTE:  What's the relevance?

18          THE COURT:  First of all, to the extent that you

19     sought to use 3500 material, it was not proper use of that

20     material.  To the extent that you have any additional

21     questions, again, what's the relevance of those questions?

22          MR. SCHULTE:  I just had two questions, one that I had

23     already asked, but it was what the AFD determination was about

24     whether the backups were involved.

25          THE COURT:  And that is totally hearsay, so you may

1    not.  We're done with AFD.

2         All right.  I'll reserve judgment.

3         Mr. Lockard, I did say does anyone have anything else.

4    Did you have something else?

5         MR. LOCKARD:  Something in the nature of flagging,

6    your Honor, for the cross this afternoon.  I think it's

7    highlighted both by what I think is the defendant intentionally

8    stepping on the line this morning as well as lines of cross

9    that he has used with expert witnesses.  There is an order

10   pursuant to Section 6 scoping out what types of

11   cross-examination is appropriate with respect to CIA tools and

12   operations.  And given the history of cross so far, we're

13   concerned that that line is going to be stepped on as well this

14   afternoon.

15        THE COURT:  And to the extent that you can elaborate

16   or point me to a particular order so I can review it over the

17   break.

18        MR. LOCKARD:  The January 30, 2020, CIPA Section 6

19   order.

20        THE COURT:  All right.

21        Mr. Schulte, you should remember it.  If not, you

22   should --

23        MR. SCHULTE:  I'm not sure what they're referring to

24   or what issues that they think have been raised by the cross.

25   I mean the only -- I'm just going through the tools

M6s5sch4

1    specifically that the government is alleging are NDI from the

2    MCC counts, which is going to be Bartender and Hickok stuff.

3    That's it.

4             THE COURT:  All right.  Well, I don't know if you can

5    get to the SCIF to refresh your recollection about what was in

6    that order, but if not, certainly you should adhere to it

7    regardless, and I'll review it over the break.

8             I'll see you, please be back in the courtroom, at

9    12:15 so we can be ready to go.

10            Thank you.

11            (Luncheon recess)

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1                           AFTERNOON SESSION

2                              12:15 p.m.

3                  THE COURT:  Should the witness be present for -- I

4     wanted to circle back to the discussion we were having before.

5                  MR. LOCKARD:  I think the witness should probably step

6     down.

7                  Mr. Weber, do you mind stepping outside for a moment?

8                  (Witness steps down)

9                  THE COURT:  So on the Hickok front, I think there are

10    three separate issues; one is relevance, one is CIPA, and is

11    essentially the nexus between this witness's testimony and the

12    defendant acknowledge, which I suppose relates to relevance.

13                 I am inclined to think that if Mr. Schulte wants to

14    take the stank and testify that in 2018 he believed that, based

15    on his work at the CIA that Hickok would have been taken down,

16    that that would be relevant and -- or would possibly be

17    relevant.  There is some uncertainties in the law in this area

18    that we are not quite at the point of discussing, but I am

19    inclined to think that he should be permitted to testify to

20    that effect.  But, I think that there are two other issues, one

21    is whether this witness, whether he can basically do that

22    through this witness, that is to say, establish that there was

23    a standard operating procedure given my understanding that this

24    leak was unprecedented.  I am not sure that it could be -- that

25    there is any foundation to establish that there was a standard

1          procedure in these circumstances, let alone a procedure that

2          would have applied a year-plus later; and second, I don't know,

3          and I am trying to be discreet hear, but if the particulars of

4          what the government did or didn't do in response to the leak,

5          if those are classified and would have been subject to CIPA

6          litigation.  I guess my inclination is to think that this is

7          not the proper witness to go there with and that again,

8          Mr. Schulte, subject to the CIPA question, if Mr. Schulte

9          wishes to take the stand and testify that based on his

10         understanding of what would likely have happened in the wake of

11         this leak, even though he wasn't there at the time, that he

12         believed that Hickok would no longer be operational, that you

13         would be permitted to do that.  But, that's sort of where I

14         think I come out on it.

15                  Mr. Lockard, anything you wish to say?

16                  MR. LOCKARD:  Your Honor, I think the government

17         agrees with exactly the analysis the Court just laid out.

18                  THE COURT:  Mr. Schulte -- or, let me modify that a

19         little bit.

20                  I'm not sure whether Hickok was taken down or

21         precisely what steps the CIA took at the time.  I'm not even

22         sure those would be relevant let alone that it is appropriate

23         to elicit those through this witness but would it be

24         appropriate to allow Mr. Schulte to ask a question of this

25         witness saying was there standard operating procedure with

1    respect to a leak of this nature in terms of what would be

2    taken down?  Not taken down?  What is your thought to that?

3              MR. LOCKARD:  I think the answer is no.  If the

4    witness is not going to be able to testify about what that

5    standard operating procedure was for all the reasons the Court

6    just laid out, then a yes-or-no answer (a) doesn't advance the

7    ball; and (b) potentially creates confusion in the jury's mind.

8              THE COURT:  Well, I think if the answer is yes

9    presumably the follow-up would be what was it and that runs

10   into the CIPA question, whether that would be classified.

11             MR. LOCKARD:  And I think even before you get to the

12   CIPA question we still think the first hurdle is still the

13   relevance question, which is what relevance does this witness's

14   understanding of whether there was or was not an SOP and what

15   it did or didn't include, especially as the Court noted, the

16   compromise of your entire development network, there is reasons

17   to think that is not a standard event.  There are a lot of

18   inferential steps that make this testimony essentially

19   speculative as to Mr. Schulte's state of mind.

20             THE COURT:  Mr. Schulte?

21             MR. SCHULTE:  I think there are several issues here.

22             I think there is a difference between the shutdown of

23   Hickok or the standard -- and the standard operating procedure

24   line of questioning.  The witness has already testified that

25   DevLAN was shut down and so I think there is two kinds of line

1    of questioning from the standard operating procedure.  I think

2    the point is establishing that this -- that the CIA has

3    procedures for doing so and that that's wouldn't be classified

4    or taking it off-line.  The second thing is it could also be

5    specifically asking about standard operating procedure and the

6    field of security that has nothing to do with the CIA at all.

7              So I think there is two sets of questions there.  The

8    CIA would have procedures with the larger question that can

9    simply be asked is, are there standard operating procedures

10   related to security incidents in general and asking about that,

11   because that's where the CIA policy comes from, it comes from

12   the larger -- I mean, it is not that hard to imagine why this

13   is the standard procedure.  If something happens, you don't

14   know what happens, so you disconnect everything and you try and

15   figure it out.  I mean, that's the -- any time there is any

16   kind of exploitation -- it doesn't have to be from the CIA,

17   from Microsoft, from anywhere -- this is the standard operating

18   procedure.  So I think if the Court is -- if the government is

19   concerned about classifications for CIA specific, that I should

20   at least be allowed to go into the standard procedure from the

21   field of security in general.

22             THE COURT:  Well, two problems.  One is that's really

23   trying to use this witness as an expert; second, I think that

24   is one further inferential step away from your own knowledge,

25   so while I think, again, you can take the stand and testify

1      that you subjectively believe that Hickok would have been taken

2      down for reasons that you can perhaps explain, I don't think

3      that you can basically use this witness to introduce or suggest

4      what your state of mind was a year-plus later.  So I will not

5      allow it further with this witness, which is not to say the

6      general subject is off limits.

7              The only other question before we resume, I did pull

8      the CIPA decision that you referred to, Mr. Lockard, but is

9      there a particular page or portion that you want to draw my

10     attention to?

11             Why don't we get the witness in while you are doing

12     that.

13             MR. LOCKARD:  While we are pulling up that page cite,

14     the subject matters it relates to is the Court's CIPA ruling

15     with respect to cross-examination about tool details and about

16     operational details, which are questions that have come up on

17     cross-examination of government experts and didn't go anywhere

18     for other reasons, but we are in a slightly different posture

19     here.

20             THE COURT:  If you can find the actual pages that

21     would be helpful, but in the meantime we will get the jury and

22     proceed.

23             Have a seat, Mr. Weber.

24             MR. LOCKARD:  We can also give the Court an update

25     about the transcript issue while we are waiting.

1          THE COURT:  We are not waiting, so.

2          THE DEPUTY CLERK:  Jury entering.

3          (Continued on next page)

M6sWsch4                         Weber - Cross

1            (Jury present)

2            THE COURT:  You may be seated.  Welcome back, ladies

3     and gentlemen.  Sorry to keep you waiting there.  We had to

4     deal with a couple matters.  We will pick up where we left off

5     with cross-examination of Mr. Weber.

6            You may remove your mask, Mr. Weber.  I remind you

7     that you are under oath.

8            Mr. Schulte, you may proceed.

9            Actually, let me ask the first question.  Before you

10    broke you were testifying about version control and Confluence

11    and Stash.  Can you just elaborate, sort of explain what your

12    answer it had to be with Git version control and that

13    Confluence had version control.  Can you just elaborate what

14    you meant by those two things?

15            THE WITNESS:  Yes, your Honor.

16            It is a significant nuance.  So when you make changes

17    in Confluence, every single change you make is tracked so you

18    could look through the history of a page and see this person

19    made this change and exactly what they changed so if you wanted

20    to undo something, you know, if a word was misspelled or

21    something like that, you could easily look through the history

22    of a document and be able to, like, either revert back to it or

23    change it.

24            Stash, itself, didn't have the same idea of version

25    control but Stash was a presentation layer for source control

M6sWsch4                          Weber - Cross

1    technology called Git that we were using.  Git, itself, is what

2    had the unique version control.  So there is some nuance in

3    that Confluence specifically had version control, Stash was a

4    presentation layer that allowed you to see the version control

5    that the Git tool allowed you to have.

6              Does that answer that?

7              THE COURT:  Somewhat.

8              THE WITNESS:  Sorry.

9              THE COURT:  That's fine.

10             Go ahead, Mr. Schulte.

11             MR. SCHULTE:  We will go into some questions to help

12   clear that up, I think.

13   BY MR. SCHULTE:

14   Q.  So as you were saying, you were describing Stash as a

15   presentation level, right?

16   A.  It handled presentation and access to projects.

17   Q.  But essentially the underlying data behind Stash is Git --

18   Git data, correct?

19   A.  A significant portion of it, correct.

20   Q.  All the source code, the source repositories are

21   represented in Git, correct?

22   A.  Correct.

23   Q.  And through Git, Git handles the version control, correct?

24   A.  That is correct.

25   Q.  So if you are writing, you are writing software, you make

M6sWsch4                         Weber - Cross

1      changes to a file, you save it, you commit it, then that

2      modification is stored into Git, correct?

3      A.   That is correct.

4      Q.   And then someone else looks at the code and says this is

5      terrible, they can click "revert" to go back to an older

6      version, correct?

7      A.   That is the simplified version but generally speaking, yes.

8      Q.   And through Git you can go through the entire iteration of

9      all the files, correct?

10     A.   I believe so.

11     Q.   Even files that have been deleted, you can go back and view

12     what they were before they were deleted, correct?

13     A.   Typically.

14     Q.   So even though Stash and Confluence are different, they

15     still rely upon some iteration of version control, correct?

16     A.   That is correct.

17     Q.   So I'm going to show you what is in evidence as 120

18     seven-29.  These are the Confluence backup files, correct?

19     A.   I am not 100 percent certain of looking at it.  It seems

20     like it could be.

21     Q.   You can look at the top where it shows where it is coming

22     from, the time stamps and see if that refreshes your

23     recollection about that.

24     A.   It looks --

25               MR. LOCKARD:  Objection.

M6sWsch4                        Weber - Cross

1          THE COURT:  Overruled.

2   A.  It looks accurate.

3   Q.  And just, you know, so that we are clear on the way this

4   version control system works, at the very bottom we see a March

5   2, 2016 backup, right?

6   A.  Yes.  All the way at the bottom there.

7   Q.  Let's see if we can --

8          THE COURT:  Can I just clarify?  Is the version

9   control the same thing as the backups?

10         THE WITNESS:  It is not.

11         THE COURT:  Can you explain the relationship between

12  those two things?

13         THE WITNESS:  So version control, the intention is to

14  be able to undo changes so if you make a mistake -- if you make

15  a mistake, you could revert back to an old one.  It is not

16  meant to protect you from the total data loss, that is what a

17  backup is meant to do.  So a backup, it being done properly, is

18  meant to protect you from if the computer breaks down and no

19  longer is able to be used, if the building were to catch fire

20  and everything were to be destroyed, if you are doing your

21  backups properly you have a copy of the data somewhere else.

22  Typically speaking, backups are only meant to be used in

23  disaster recovery situations.  Version control is meant to be

24  used in a day to day-type of operation where you want to be

25  able to, like I said, if somebody made a mistake or you don't

1    like the direction a document is going, you can go back to an

2    older version.

3    Q.  So if there is an issue and the Confluence server failed,

4    you don't have access to the version history anymore, correct?

5    A.  That would be correct.

6    Q.  And that's because the data is gone, right?

7    A.  That's correct.

8    Q.  So if the data is completely gone then that's when you look

9    to these backups, correct?

10   A.  That's the theory, yes.

11   Q.  And then you would theoretically restore to a working copy,

12   correct?

13   A.  Correct.

14   Q.  And, once again, you would have access to the version

15   control, right?

16   A.  That is correct.

17   Q.  So due to the way version control works, this last backup

18   file mentioned -- this last backup file here would contain the

19   data from the previous files, correct?

20   A.  Potentially.  I don't know the nuance of Confluence's

21   version controlling.  I don't know if deleted pages would be

22   under version control, stuff like that.

23   Q.  So you are not familiar with how Confluence handles that?

24   A.  Not intimately familiar.  I occasionally would go back to

25   an old page but I am not familiar with how it handles all the

1    different scenarios of modification to a page.

2    Q.  What about the Stash?  Are you more familiar with that?

3    A.  I am more comfortable with it but definitely, again, I

4    can't speak to the nuance of when something would fall out of

5    version control and when wouldn't.

6    Q.  OK.  But the idea and the way version control is set up is,

7    from your experience, you are able to go back to deleted files,

8    correct?

9    A.  In Stash -- in Stash, definitely I remember having done

10   that.  I don't know if Confluence, if you deleted a page if the

11   version control in Confluence would cover that.

12   Q.  To move on to talk a little bit about classified

13   information in general, there are three levels of

14   classification, correct?

15   A.  There is three levels of classified material.

16   Q.  And when you start at the CIA you have several weeks of

17   training when you start, right?

18   A.  There is a significant amount of training when you start at

19   the agency.

20   Q.  And every CIA officer is what is called a derivative

21   classifier, correct?

22   A.  I believe that would be correct.

23   Q.  A derivative classifier is someone who has the authority to

24   classify documents, correct?

25   A.  The derivative classifier is somebody who has the authority

1    to apply classification decisions based on guidance.

2    Q.   So you used -- the CIA provides reference material that you

3    use when you are determining classification, correct?

4    A.   Correct.

5    Q.   And the classified document is marked with a specific

6    classification reason and other information, right?

7    A.   If being done properly.

8    Q.   So when you write something, ultimately you make the

9    determination of whether or not it is classified, correct?

10   A.   Again, you are not making a determination, you are applying

11   what has been determined as classified or not.

12   Q.   Well, you are applying the guidelines that you view them to

13   be, right?

14   A.   As they're laid out, correct.

15   Q.   Is your decision a final classification decision?

16   A.   There are prescribed ways that classification can go under

17   review, either because something is misclassified, the person

18   made the wrong interpretation, or because the information is no

19   longer deemed classified.  But there are official ways of

20   handling that.

21   Q.   And as applied, like you said, so if people disagree with

22   each other's classifications something like this would apply,

23   right?

24            MR. LOCKARD:  Objection.

25            THE COURT:  Overruled.

1   A.   The -- if somebody felt that something was misclassified

2   then it would be brought to the attention of an officer whose

3   job it is to review those classification decisions.

4   Q.   And there is the developers are not those classification

5   experts, correct?

6   A.   To my knowledge that is correct.

7   Q.   The CIA has classification experts, right?

8   A.   That is correct.

9   Q.   An entire group of classification experts, right?

10  A.   I don't know the size or scope of the experts.

11  Q.   But you never worked in that group, right?

12  A.   That is correct.

13  Q.   And you are not authorized by the CIA to conduct

14  classification reviews of other people's submissions, right?

15  A.   That -- every agency officer is responsible for the

16  protection of classified information so if somebody said

17  something was unclassified and I felt that it was classified, I

18  would have the responsibility for flagging that and upping the

19  classification.

20  Q.   Well, you would flag it for somebody else to review whether

21  it is classified, right?

22  A.   It would probably, generally speaking, you would usually

23  discuss it with the person who made the original classification

24  decision.  If there was still a disagreement then, yes, you

25  would kick that over to the next -- the experts, essentially.

M6sWsch4                          Weber - Cross

1    Q.   And do you know what the PRB is?

2    A.   The publication review board, I assume?

3    Q.   Yes.

4    A.   Yes, I am familiar with it.

5    Q.   And what is it?

6    A.   So anything that an agency officer writes for publication

7    in the public should go through review in the PRB.  This could

8    be academic papers if they're going through college, it could

9    be résumés, things like that.  People write memoirs sometimes.

10   It is an official review to make sure that it is not classified

11   and that classified information isn't contained.

12   Q.   And there is a whole process for that, correct?

13   A.   I assume.  I have never had to go through the PRB.

14   Q.   Not even for your résumé?

15   A.   I do not have -- I have not created a résumé since going to

16   the Agency.

17   Q.   But it is fair to say that once the PRB makes its decision,

18   you don't have authority to overrule the PRB, right?

19   A.   I -- I wouldn't -- I would assume not.  I don't know, I

20   have never -- never really thought or, like, looked into it.

21   Q.   So is it fair to say that the work that was done in CCI was

22   offensive work, correct?

23   A.   The -- within CCI all matters of work were conducted.

24   Q.   Specifically with EDG?

25   A.   Within EDG our focus was offensive cyber capabilities.

1    Q.  And the point of this -- the ultimate end goal for the

2    development of the cyber capabilities are to steal secrets,

3    correct?

4              MR. LOCKARD:  Objection.

5              THE COURT:  Sustained.

6    Q.  Well, there is a common saying within -- there is a common

7    way saying of what the CIA is trying to do, right?

8              MR. LOCKARD:  Objection.

9              THE COURT:  Sustained.

10   Q.  The point is to gather intelligence for the policy makers,

11   right?

12   A.  The Agency's mission is outlined in 12333, executive order

13   12333.  I don't know the exact reason for what we are supposed

14   to do, just what our mission is.

15   Q.  But within EDG there was no software development to protect

16   the U.S. from incoming attacks, right?

17             MR. LOCKARD:  Objection.

18             THE COURT:  Sustained.

19   Q.  Are you familiar with the NSA?

20   A.  Yes.  I know what the NSA is.

21   Q.  So the NSA is largely tasked with defensive capabilities,

22   correct?

23             MR. LOCKARD:  Objection.

24             THE COURT:  Sustained.

25   Q.  I want to discuss the classified information that I was

1    exposed to or was available to me at the CIA.  You are aware of

2    several tools and operations that I worked on, right?

3    A.   I am -- I would be aware of some, correct.

4    Q.   And throughout those operations I learned highly classified

5    information, right?

6    A.   I would assume, but I don't know the specifics.

7    Q.   You are familiar with ▮▮▮▮, correct?

8           MR. LOCKARD:  Objection.

9           THE COURT:  Sustained.

10   Q.   You are aware of countless projects I worked on for

11   counterterrorism, correct?

12   A.   I don't know if countless would be the correct term but I

13   did work on projects that supported the CT mission.

14   Q.   What would you define it to be?

15   A.   I was not keeping a close count of what you were working on

16   but fortune one for sure.

17          MR. SCHULTE:  All right.  I think I'm going to move to

18   introduce stipulation 3010.

19          MR. LOCKARD:  No objection.

20          THE COURT:  All right.  You may proceed.

21   BY MR. SCHULTE:

22   Q.   This is Government Exhibit 3010:

23          As a result of the defendant's employment at the

24   Central Intelligence Agency, he was privy to and remains aware

25   of sensitive national defense information beyond what he is

1      charged with disclosing or attempting to disclose in this case,

2      the disclosure of which would be extremely damaging to national

3      security.

4               I will move on to Government Exhibit 806.  I think you

5      testified about this on direct, right?

6      A.   That's correct.

7      Q.   I am going to show the witness what's marked as Defendant's

8      Exhibit 806.  Does this appear to be the same document you

9      reviewed earlier?

10              MR. LOCKARD:  Objection.

11              THE COURT:  Sustained.

12     Q.   Do you recognize what this document is?

13     A.   It appears to be the same.

14     Q.   What is it?

15     A.   The cover of a notebook.

16              MR. SCHULTE:  I move to introduce Defendant's Exhibit

17     806.

18              MR. LOCKARD:  Objection.

19              THE COURT:  Mr. Schulte, are you offering the entirety

20     of?

21              MR. SCHULTE:  No.  These are sections that were pulled

22     and provided to the government.

23              THE COURT:  I understand.  Is it a 38-page document

24     that you have here?

25              MR. SCHULTE:  This is -- there is 38 pages, yes.

1            THE COURT:  The objection is sustained.

2    BY MR. SCHULTE:

3    Q.  I'm going to show what's marked as Defendant's Exhibit

4    806-1.  Do you recognize this?

5    A.  I appear to be looking at the same thing I just looked at.

6    Q.  And what was it?

7    A.  The cover of a notebook.

8            MR. SCHULTE:  I move just to introduce this 806-1

9    which is the front two pages.

10           MR. LOCKARD:  No objection.

11           THE COURT:  Admitted.

12           (Defendant's Exhibit 806-1 received in evidence).

13   BY MR. SCHULTE:

14   Q.  So can you clearly see the date that is written on the

15   notebook in this?

16   A.  I assume the 7/2018 is a date.

17   Q.  Does that appear to be a date to you?

18           MR. LOCKARD:  Objection.

19   A.  I would assume it is.

20           THE COURT:  Ladies and gentlemen, let me just

21   interrupt to give you one quick instruction.  You will see it

22   says here "attorney-client privilege."  I don't know if you are

23   familiar with what that is but generally, under American law,

24   certain communications between a client and his or her lawyer

25   are privileged, are basically confidential and not subject to

1    disclosure.  I have made rulings in this case about certain

2    statements that Mr. Schulte is alleged to have made that are

3    admissible and some of those have come into evidence.  So the

4    fact that it says "attorney-client privilege" here, you should

5    just understand I have previously made rulings that what you

6    are seeing in these notebooks is admissible and you may,

7    therefore, consider what weight, if any, you put on the

8    exhibit, it is yours to make, and what weight, if any, you put

9    on the fact that it is labeled attorney-client privilege is a

10   decision for you to make, but I instruct you that, as a matter

11   of law, the things that have been admitted into evidence are

12   not privileged or the privilege has been waived so they are

13   admissible.

14            You may proceed, Mr. Schulte.

15   BY MR. SCHULTE:

16   Q.  And you also see next to the date it says 80 sheets, right?

17   A.  Yes, I do see that.

18   Q.  So, in total, that's 160 pages front and back, right?

19   A.  I assume.  Yes.

20   Q.  And you were asked to review one page, right?

21   A.  I don't recall, specifically, how many pages I was asked to

22   review.

23   Q.  Let's pull that up, Government Exhibit 806.  You testified

24   about this on direct, right?

25   A.  Yes.  That is correct, I believe.

1    Q.  So at this point in 2018 WikiLeaks has my source code

2    correct?

3    A.  The WikiLeaks had been publishing stuff at that point.  I

4    don't know -- I don't know what WikiLeaks had or didn't have.

5    Q.  But you are aware that the agency determined that both

6    Stash and Confluence, at least, were taken; correct?

7              MR. LOCKARD:  Objection.

8              THE COURT:  Sustained.

9    Q.  At this point in 2018 you testified that you are aware that

10   WikiLeaks published information from Confluence and Stash,

11   right?

12   A.  That is correct.

13   Q.  It is fair to say that the software that parses NTFS and

14   EXT3 is not classified, correct?

15   A.  I -- I would not make that statement.

16   Q.  You would say that NTFS parsers are classified?

17   A.  The classification decisions, like it depends, like any

18   classification decision, it depends on the specifics so I can't

19   make general statements about classification.

20   Q.  Well, I am talking about not related to deployments or

21   actually using any tool, I am just talking about software that

22   parses NTFS.

23   A.  Again, the specifics matter.

24   Q.  What specifics do you think that would depend on?

25             MR. LOCKARD:  Objection.

M6sWsch4                           Weber - Cross

1          THE COURT:  You can answer in a general way, if

2     possible.  If not, then you should tell me.

3          THE WITNESS:  Generally, how we arrived at the

4     capability, how it was written, when it was written, and where

5     it was received from would inform a classification decision.

6     BY MR. SCHULTE:

7     Q.   OK.  Do you know if Microsoft Windows parses NTFS?

8     A.   Yes, it does.

9     Q.   And Microsoft Windows can be bought by anyone in the

10    general public, correct?

11    A.   The software you mean?

12    Q.   Yeah.

13    A.   Yes.  Generally, I believe anybody can purchase Windows.

14    Q.   And what about Apple?  Does Apple's operating system parse

15    EXT3?

16    A.   I don't know, actually.

17    Q.   Can anyone buy Apple's operating system?

18    A.   I don't think you can buy the operating system, but.

19    Q.   You can't go out and buy OSX whatever?

20    A.   I think it's baked into the machine you buy.

21    Q.   OK.  But it is safe to say that at least with Windows, or

22    even buying Apple products, that there exists software that

23    parses NTFS that is not classified, right?

24    A.   That is correct.

25    Q.   So looking at this page here and the fact that I developed

1    software to parse Microsoft or to parse NTFS and EXT3, you

2    don't know whether that software would be classified from that,

3    right?

4    A.   Again, details matter, but I'm working under the assumption

5    that this is in reference to code you wrote while at the

6    Agency.

7    Q.   OK, but the description here, the fact that the CIA or a

8    developer from the CIA wrote something that parses NTFS or EXT3

9    in general is not classified, right?

10   A.   Again, it depends on the details.  I think generally

11   stating that a CIA officer may parse NTFS is not a classified

12   statement.

13   Q.   OK.  And that would be the same thing for general use

14   software like -- or -- I'm sorry -- general use C++ data

15   structures or something, right?

16   A.   Again, depending on the level of detail and the context,

17   it's hard to speak to what is classified and not.

18              THE COURT:  Can you just translate for us what parsing

19   NTFS" what that means?

20              THE WITNESS:  Sure.  In layman's terms the parsing a

21   file system would be like to look at it in generalities as

22   think of it almost like opening up a book with a table of

23   contents.  The NTFS -- the file system -- isn't generally laid

24   out in sequential order so you would often have to look up

25   information about the file to find out exactly where on a hard

1    disk that information is.  So again, think of it kind of along

2    the lines of looking at a table of contents and then knowing,

3    OK, I have to go to page 10 to read the thing that I am looking

4    up.

5    BY MR. SCHULTE:

6    Q.  But data structures, like an ArrayList, the fact that

7    developers use this in general wouldn't be classified, right?

8    A.  Simple programming statements like that, in generalities,

9    probably would not be classified.

10   Q.  And you were shown only three pages of this notebook,

11   right?

12            MR. LOCKARD:  Objection.

13            THE COURT:  Sustained.

14   Q.  Well, there is the front cover, right?  And you were asked

15   about this on your direct, right?

16   A.  Correct.

17            THE COURT:  Showing the first page of Government

18   Exhibit 806 after the cover.

19   Q.  And you only testified about this page in this document,

20   right?

21   A.  I testified about this page, correct.

22   Q.  Do you recall reviewing any other pages of this notebook?

23   A.  I have seen other pages of this notebook.

24   Q.  You have been shown or you have been provided all the other

25   notebooks to read through?

M6sWsch4                           Weber - Cross

1    A.   No.   That is not correct.

2    Q.   The prosecutors picked out pages that they wanted you to

3    review?

4               MR. LOCKARD:   Objection.

5               THE COURT:   Sustained.

6    Q.   You weren't given the notebook to take home and review,

7    right?

8    A.   That is correct.

9    Q.   They asked you to review certain pages of it, right?

10   A.   They gave me specific snippets and asked questions about

11   them.

12              THE COURT:   "They" being the prosecutors?

13              THE WITNESS:   The prosecutors, I believe -- yeah,

14   exclusively the prosecutors.

15   Q.   I'm not talking about just in your testimony but through

16   all your meetings with them in general.

17   A.   Correct.

18   Q.   OK.

19        I want to pull up what is in evidence as Government Exhibit

20   616.   I'm sorry -- yeah, 616.   Do you recognize this?

21   A.   I don't know if I have ever seen this before.

22   Q.   You know what Hickok is though, right?

23   A.   I know a definition of Hickok, yes.

24   Q.   You know a general user's guide is, right?

25   A.   I can make assumptions.

1    Q.   What is the date that you see here?

2    A.   2 August 2014.

3    Q.   This is a 35-page document, right?

4    A.   Based on what the PDF shows up top it says 35 pages.

5    Q.   And it has been labeled unclassified, correct?

6    A.   That is the classification I see on the document.

7    Q.   And the dissemination is FOUO, correct?

8    A.   Correct.

9    Q.   And that just means for official use only, right?

10   A.   That's correct.

11   Q.   And that's a dissemination control, correct?

12   A.   That is correct.

13            THE COURT:  Can you just explain what dissemination

14   control is as opposed to classification level?

15            THE WITNESS:  My understanding of it, it is

16   classification makes a statement about level of potential

17   damage to the U.S. government.  Dissemination is meant to help

18   understand who should be accessing the information.

19            THE COURT:  So something can be limited for official

20   use only but not classified; is that an accurate statement?

21            THE WITNESS:  I think the only time FOUO is applied is

22   to classified information.

23            THE COURT:  Because classified information is, by

24   definition, for official use?

25            THE WITNESS:  Yes.  That would be my understanding.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

1   BY MR. SCHULTE:

2   Q.  And you are aware that WikiLeaks released information about

3   Hickok, correct?

4   A.  No, that is not correct.

5   Q.  WikiLeaks did not release any information about Hickok?

6   A.  I was not aware of if Hickok was involved in the WikiLeaks

7   releases.

8           MR. SCHULTE:  I would like to read in another

9   stipulation, Government Exhibit 3009.

10           MR. LOCKARD:  No objection.

11           THE COURT:  OK.  You may proceed.

12           MR. SCHULTE:  The following statements appear in the

13   WikiLeaks Vault 7 release:  Hickok, used for transferring tools

14   and their associated documentation between DevLAN and COG

15   network consists of two firewalls, a data store that houses the

16   files to be transferred, and the Jira instance for discrepancy

17   reporting.

18           The operators also have an instance of Stash in the

19   COG network, however syncing between the two instances would

20   not be possible without changing the location of the operator's

21   version.  It may be possible to relocate the operator's Stash

22   instance to Hickok, which would allow syncing with AED's

23   version of Stash, similar to how the Jira instance worked

24   today.

25           In EDG, we use Jira to track issues on projects.  Jira

1    sits on Hickok which is shared between us and COG.

2              And the following image appears in the WikiLeaks Vault

3    7 release:

4              Should I describe it?

5              THE COURT:  It is in evidence.  The jury can see it

6    now and the jury will have it in the jury room during their

7    deliberations.

8    BY MR. SCHULTE:

9    Q.  I think you also testified about Government Exhibit 809,

10   correct?

11   A.  I don't recall the exhibit numbers.  I would have to see

12   it.

13   Q.  OK.

14             THE COURT:  Can I just clarify while we are getting

15   that?  The information in that stipulation that Mr. Schulte

16   just read, is it correct to say you didn't know one way or

17   another whether that was in the WikiLeaks leak?

18             THE WITNESS:  That is correct.

19   BY MR. SCHULTE:

20   Q.  This was the notebook that you testified to on direct,

21   right?

22   A.  This one appears to have a different cover page.

23   Q.  OK.  Do you recognize this?

24   A.  Yes, I recognize this page.

25   Q.  I am just going to show the witness and the parties what is

1    marked as 809-1.  Do you recognize this?

2    A.   This appears to be the same notebook page from -- that you

3    just showed me.

4              MR. SCHULTE:  I move to introduce 809-1.

5              MR. LOCKARD:  Objection.

6              THE COURT:  Ground?  You said objection?  Or no

7    objection?

8              MR. LOCKARD:  Based on the material at the bottom of

9    page 2.

10             THE COURT:  I am going to admit it but direct that

11   that be redacted before the second page is shown to the jury.

12   So with that caveat, it is admitted and you may display page 1

13   for now.

14             (Defendant's Exhibit 809-1 received in evidence)

15   BY MR. SCHULTE:

16   Q.   Is it easier to read this page?

17   A.   I am still looking at the notebook cover.

18   Q.   Is it easier to read the notebook cover?

19   A.   It doesn't -- it doesn't make it harder or easier.

20   Q.   Do you see a date on this notebook?

21   A.   Potentially.

22   Q.   OK.

23   A.   7/25.

24   Q.   OK.

25             Let's go back to Government Exhibit 809.  And the

1    government had you read around the page here, right?

2    A.   They asked me to read that first statement.

3    Q.   What is the date listed there?

4    A.   It appears to be Wednesday, 8/8.  I don't know if that's

5    2016 or 2018.

6    Q.   The statement that you read, you testified it starts out:

7    If the government doesn't pay me $50 billion in restitution and

8    prosecute the criminals, right?

9    A.   I wasn't able to read the second word but I think that's

10   what I read the rest of it as.

11   Q.   So this statement here, it doesn't say anything about

12   releasing classified information, right?

13          MR. LOCKARD:  Objection.

14          THE COURT:  It speaks for itself.  Next question.

15   Q.   Can you read the middle of the page there?

16   A.   The portion that's below the Wednesday 8/8?

17   Q.   Yes; the portion you didn't read.

18   A.   They called me down at 6:00 a.m. for my 2:00 Court.  From

19   6:00 to 10:00 a.m. I did nothing down there.  Finally brought

20   me back.  I took my last piece and I'm feeling great.  I

21   envisioned my appointment as a cardinal and becoming the -- I

22   don't recognize -- something-something -- as I unified

23   Christianity around the church.  Took too much and feel sick.

24   Q.   Would those words be "young Pope"?

25          MR. LOCKARD:  Objection.

M6sWsch4                          Weber - Cross

1          THE COURT:  Sustained.

2    Q.  It's fair to say that you don't know my state of mind when

3    writing the document, right?

4    A.  That's a fair statement.

5    Q.  I think there were other pages in the notebook that you

6    testified about, right?  This page 10 in GX-809?

7    A.  Is that what I am looking at right now?

8    Q.  Yes, it is.

9    A.  I believe, yes, this was a page that I was asked to read.

10   Q.  And the prosecutors had you focus on these sentences,

11   right?

12   A.  I, if I recall correctly, it was the top left-hand corner.

13   Q.  Yes.

14        It is fair to say that you have never read these statements

15   on Twitter, right?

16   A.  That's correct.

17   Q.  You didn't read it from the internet, correct?

18   A.  I lost the page but --

19   Q.  I just took it down.

20   A.  OK.

21   Q.  I can pull it back, but --

22   A.  No.  That is correct, though.

23   Q.  But the page showed cross-outs and Scribbles and stuff

24   written all over the page, right?

25   A.  You took the page away from me.

M6sWsch4                        Weber - Cross

1    Q.   OK.  I will get it back for you.  Sorry.

2    A.   There are cross-outs and Scribbles, correct.

3    Q.   And again, you don't know my state of mind when this was

4    written, correct?

5    A.   That is correct.

6    Q.   And this was never publicly disclosed, correct?

7              MR. LOCKARD:  Objection.

8              THE COURT:  Sustained.

9    Q.   Through your experience at the CIA, the CIA has never

10   deliberately exposed sensitive national defense information,

11   correct?

12             MR. LOCKARD:  Objection.

13             THE COURT:  Sustained.  You know what?  I will allow

14   it.

15             In your experience at the CIA, has the CIA ever

16   deliberately exposed such information?

17             THE WITNESS:  I am not aware of a scenario where we

18   have deliberately exposed sensitive -- I'm not aware of any

19   scenario like that.

20             THE COURT:  Ladies and gentlemen, just a reminder, I

21   think I told you a week or two ago that national defense

22   information is a legal term that I will give you further

23   instructions about at the conclusion of the case.  The witness

24   is not testifying about that legal term, *per se*, but just those

25   words in a colloquial sense.

1          Go ahead.

2    BY MR. SCHULTE:

3    Q.  You read here information that was about Bartender,

4    correct?

5    A.  I read information that you wrote about Bartender, correct.

6    Q.  And at the time that this was written in August or -- at

7    the time this was written in 2018, Bartender no longer was

8    used, correct?

9    A.  I am not aware if that is an accurate statement or not.

10   Q.  I thought you testified on direct that the tools were shut

11   down from DevLAN.

12   A.  At the time there was a standdown on tools.  I don't know

13   what the decisions were years later.

14   Q.  You work at the CIA still, right?

15   A.  That is correct.

16   Q.  So you would not know if any of those tools were being

17   used?

18          MR. LOCKARD:  Objection.

19          THE COURT:  Overruled.

20   A.  I was in a new position in 2018.  My need to know about the

21   Bartender suite would no longer be relevant so I was not -- I

22   was not aware of what decisions were being made around it.

23   Q.  Well, before you left EDG there was still a standdown on

24   the tools, right?

25   A.  I don't know.  Again, it's a specific details matter, so.

M6sWsch4                        Weber - Cross

1    Q.  OK.  If a tool is exposed, that tool is not generally used

2    again, right?

3                MR. LOCKARD:  Objection.

4                THE COURT:  I'll allow it.

5    A.  The deployment of tools always involves risk and the risk

6    decision surrounding that is COG's domain so they would be the

7    one making the final statement on if a risk of using an exposed

8    tool was required for mission.

9    Q.  But EDG remained equity holders for a lot of that code,

10   right?

11   A.  EDG would -- EDG's responsibility was to help inform COG on

12   what risks were being taken technically.

13   Q.  So your testimony is if a specific tool was outed as a CIA

14   tool it would still be used, potentially?

15                MR. LOCKARD:  Objection.

16                THE COURT:  Sustained.  Asked and answered.

17   Q.  And Bartender was actually exposed long before WikiLeaks

18   exposed it, right?

19   A.  Exposed is -- exposed is probably not an accurate term.  As

20   we discussed earlier, it had been caught but in terms of being

21   outed as a CIA tool, to my knowledge, it had not been exposed

22   as a CIA tool.

23   Q.  But the functionality had been exposed such that it was not

24   used again, right?

25                MR. LOCKARD:  Objection.

M6sWsch4                         Weber - Cross

1          THE COURT:  I think the question -- let me translate

2    the question:  After it was -- sorry.

3          Was the functionality revealed in the vendor report

4    you testified about earlier?

5          THE WITNESS:  A portion of the functionality was

6    revealed.

7          THE COURT:  After that happened, was the tool -- did

8    the CIA continue to use the tool?

9          THE WITNESS:  I don't know -- I don't know yes or no

10   to that.

11   BY MR. SCHULTE:

12   Q.   But as the lead developer on Bartender, it was required to

13   rewrite it, right?

14   A.   We did make the decision that we would do a substantial

15   rewrite of it but I don't know -- I don't know if Bartender, as

16   it stood at the time, was ever deployed again or not.

17   Q.   You testified on direct about tools being lost, right?

18   A.   I testified about the decision at the time as it was told

19   to me.

20   Q.   But you didn't need specific details when you testified on

21   direct, right?

22   A.   The statement that I testified to was that -- what occurred

23   immediately following WikiLeaks.

24   Q.   You testified on direct that disclosure on WikiLeaks gave

25   you insight into the intentions of the tool, correct?

1   A.  Potential insight, correct.

2   Q.  And how witting the asset was to deploying it, correct?

3   A.  If I recall correctly, the Bartender Document would have

4   talked to that.

5   Q.  And the Bartender Document was exposed by WikiLeaks, right?

6   A.  I believe so, correct.

7   Q.  The information specifically noted in the notebook, tool

8   described in vendor report is in fact Bartender, CIA tool set

9   for operators to configure for deployment; that statement is

10  too generic to be classified, correct?

11         MR. LOCKARD:  Objection.

12         THE COURT:  I will allow it.

13  A.  I have concerns about that statement.  I would consider it

14  to be classified because it points to an operator being witting

15  to the usage of the tool.

16  Q.  I think like you said earlier, you are not an expert in

17  classification, correct?

18  A.  I have been trained to make classification decisions on how

19  it is outlined.  I feel like the agency would that that is a

20  classified statement.

21  Q.  No.  I was saying that you testified earlier that you are

22  not a classification expert, correct?

23  A.  No, I am not a classification expert.

24  Q.  But, even so, the information here that you read, that

25  information was all released by WikiLeaks, correct?

1    A.   The information you just had me read was in your notebook.

2    Q.   Yes.   That's correct.   The question is that information

3    was -- there is no new information in that statement from what

4    WikiLeaks provided, correct?

5    A.   I would have to review what WikiLeaks put out but I

6    believe -- I believe the Bartender Document would have made

7    that statement.

8    Q.   OK.   I will move on.

9         I want to talk a little bit about physical security.   The

10   CCI office is an open CIA building, correct?

11            MR. LOCKARD:   Objection.

12   A.   I don't know actually the official, the official status of

13   the building.

14   Q.   You don't know the security code of the site?

15   A.   I do not.

16   Q.   OK.   That was easy.

17        Now I want to bring up what's in as Government Exhibit 111.

18   So, do you recognize this?

19   A.   I do.

20   Q.   What is this?

21   A.   This is the CCI office on the eighth floor.

22   Q.   And what about this?

23   A.   CCI office on the ninth floor.

24   Q.   So I just want to go through where some things are located

25   here.   Do you see where it says 9W89A?

M6s5sch4                          Weber- Cross

1    A.   I do.

2    Q.   That's a server room, correct?

3    A.   At the time of this drawing that is correct.

4    Q.   That's where the ESXi server existed, correct?

5    A.   I believe so.  That's correct.

6    Q.   And you cannot enter the server room without badging in,

7    correct?

8    A.   I believe that to be correct but I'm not 100 percent

9    certain.

10   Q.   Well, on your badge records, it will show what the room

11   number is, right?

12   A.   I believe so.

13   Q.   And then after 9E79 is another server room, correct?

14   A.   I believe that to be correct.

15   Q.   And this was the primary ISB server room, correct?

16   A.   That was my understanding but that's a better question for

17   ISB.

18   Q.   But did you know that 9E79 was where the FS-01 Stash server

19   and other infrastructure existed, correct?

20   A.   I don't know the physical locations of the new ones you

21   just described.

22   Q.   You don't know where those servers were located?

23   A.   No.

24   Q.   OK.

25            Do you see 9W85?

M6s5sch4                        Weber- Cross

1   A.   Yes.

2   Q.   And that's the men's bathroom on the floor, right?

3   A.   I think that's technically the women's bathroom.

4   Q.   What is the men's bam room?  This one?

5   A.   Correct.

6   Q.   And it is the same location on the eighth floor, correct?

7   A.   Generally speaking, yes.

8   Q.   And after returning from the bathroom you would

9   typically -- you could use one of these doors, right?  9W53A,

10  9W89?

11  A.   There were multiple ways to get into the vaults.

12  Q.   Yes, but these -- these are doors to the main vault, right?

13  A.   Well, 9W89 would lead to the 9W89 vault.  9W53 would lead

14  to the 9W53 fault.

15  Q.   9W89B connects to those two vaults, right?

16  A.   That's correct.

17  Q.   And these doors can be locked from the inside, correct?

18  A.   I assume.  That is generally how it would work but I don't

19  remember the specifics of those doors.

20  Q.   But then otherwise, as they are and you would walk around,

21  this is the front, these are the main doors to the vaults,

22  right?

23  A.   For the definition of a main entrance so, I mean, the cube

24  you see that's labeled 9E53-061 that's where the AD's assistant

25  sat so visitors would tend to go through that door to talk to

M6s5sch4                        Weber- Cross

1     her.

2     Q.  But this is the door that you would spin off when you are

3     locking the vault, right?

4     A.  Yes.  I believe that's the only -- that was the only vault

5     dial.

6              THE COURT:  Mr. Schulte, if you can just make a record

7     there?  You were referring to 9E53 but, if you can, as you ask

8     questions make a record of what you are referring to, that

9     would be great.

10             MR. SCHULTE:  OK.

11    Q.  And the eighth floor layout is largely the same, right?

12    A.  I wouldn't say largely.  There is -- there is significant

13    differences in the floor layout.

14    Q.  But you are familiar with both the floors, correct?

15    A.  It depends on your definition of familiar.  I have walked

16    through both floors.

17    Q.  AED space is on the eighth and ninth floors, right?

18    A.  General am speaking, correct.

19    Q.  The accesses to the vaults, you have to badge in; correct?

20    A.  That is correct.

21    Q.  I am going to reference that in a minute.  I am going to

22    show what is in evidence Government Exhibit 105; page 13 of

23    105.  I just want to highlight this row.  The time here shows

24    as 17:45, correct?

25    A.  For the thing that your pointer is over, that is correct.

M6s5sch4                          Weber- Cross

1    Q.   That is 5:45 p.m., correct?

2    A.   That is correct.

3    Q.   And this shows an attempted entry to 8W53A, right?

4             MR. LOCKARD:  Objection.

5             THE COURT:  Are you familiar with these records,

6    Mr. Weber?

7             THE WITNESS:  Just from, like -- I have never really

8    looked at these records.  I would just be making assumptions

9    based on what I am reading.

10            THE COURT:  All right.  So sustained.

11   BY MR. SCHULTE:

12   Q.   Does the column headers help?

13   A.   The column headers say something but I would just be

14   reading what it is.  I don't know, like -- I can't speak to the

15   nuance of what is on here.

16   Q.   During your time working at the CIA you have never seen

17   badge records before?

18   A.   Outside of, outside of this case, I don't believe so.

19   Q.   So you have seen them as part of this case, correct?

20   A.   I believe I was shown -- I was shown something that looked

21   like this before.

22   Q.   And you weren't -- you didn't learn anything or you weren't

23   able to, through your experience, determine what the records

24   represent?

25            MR. LOCKARD:  Objection.

M6s5sch4                          Weber- Cross

1            THE COURT:  Sustained.  Take this down and move to

2    your next line of questioning, please.

3    BY MR. SCHULTE:

4    Q.  I am going to talk a little bit about DevLAN and the

5    servers and services it hosted.  An ESXi server is just a

6    server of virtual machines, correct?

7    A.  An ESXi server is -- that's probably an oversimplified

8    statement, but.

9    Q.  I mean, if you would like to pose a better one or --

10   A.  ESXi is meant to virtualize a variety of network

11   applications and networking capabilities.  It does more than

12   just host virtual machines.

13   Q.  And, specifically, the ESXi server that we worked on, do

14   you know when that was purchased?

15   A.   I don't remember the specific date.

16   Q.  Do you know why it was purchased?

17   A.   I do.

18   Q.  And why was that?

19   A.  We, as I stated earlier, we wanted to be able to create

20   development tools to assist with our development environment.

21   Q.  And, initially, what types of virtual machines were set up

22   on the ESXi server?

23   A.  Again, it was testing machines, it was machines that would

24   help with the configuration of tools, compiling of tools.

25   Things like that.  It was meant to be a shared between OSB.

M6s5sch4                      Weber- Cross

1    Q.   That included things like the Doxygen server, correct?

2    A.   I believe the could Doxygen server was sitting on OSB

3    infrastructure.

4    Q.   And the same for the IRC server, right?

5    A.   I believe that to be accurate, too.

6    Q.   And I was the one -- I was the person who filed the

7    purchase order for the machine, correct?

8    A.   I don't remember.

9    Q.   Were you aware, though, that the ESXi server was part of my

10   CMR?

11           MR. LOCKARD:  Objection.

12           (Continued on next page)

13

14

15

16

17

18

19

20

21

22

23

24

25

1             THE COURT:  Do you know what CMR refers to?

2             THE WITNESS:  I do.

3             THE COURT:  What does it refer to.

4             THE WITNESS:  Well, I don't know if I know what CMR

5     stands for, but it was a -- it was how we tracked the

6     accountable property.

7             THE COURT:  All right.  Sustained.

8             MR. SCHULTE:  I'm going to show, display Government

9     Exhibit 1071.  It's in evidence.

10    Q.  Do you know what this is?

11    A.  It appears to be an email from you to Anthony.

12    Q.  OK.  And do you know the date of the email?

13    A.  It's April 21, 2016.

14    Q.  OK.  And the subject?

15    A.  CMR, transfer of equipment, especially OSB server, to OSB.

16    Q.  OK.  And you understand that when you have accountable

17    property assigned to you, there's a mechanism for transferring

18    that, correct?

19    A.  That is correct.

20    Q.  And as the CMR, as the accountable property holder, you're

21    listed as the POC for that device, correct?

22            MR. LOCKARD:  Objection.

23            THE COURT:  Overruled.  I'll allow it.

24    A.  I do not recall individuals having CMRs.  The branches --

25    the branches had CMRs, and there were POCs listed for when we

M6sWsch5                         Weber - Cross

1    were trying to find equipment.

2    Q.   OK.   But those POCs are for individuals, right?

3    A.   Typically.

4    Q.   So at what point did the Atlassian products come into

5    fruition?

6    A.   I don't remember the exact -- exact year.

7    Q.   OK.   But just to be clear, the Atlassian products we've

8    heard about a lot -- Crowd, Stash, Confluence, Jira, Bamboo --

9    right?

10   A.   Correct.

11   Q.   Those are the only Atlassian products that were used on

12   DevLAN, right?

13   A.   To my -- to my memory, correct.

14   Q.   OK.   And the individual who first set this up set it up on

15   his personal computer, right?

16   A.   I don't know.

17   Q.   You don't know where it was set up originally?

18   A.   No, I don't.

19   Q.   OK.   There came a time when the Atlassian products were

20   migrated to the ESXi server, right?

21   A.   A portion of them, Confluence and Bamboo.

22   Q.   OK.   There was excess space on the ESXi server, correct?

23   A.   That was part of the reasoning, correct.

24   Q.   OK.   And at that time I created the virtual machines on the

25   ESXi server, right?

M6sWsch5                        Weber - Cross

1    A.   I don't recall if it was you, me, or whoever.

2    Q.   You don't recall who set the Atlassian products up?

3    A.   For the original creation of the virtual machines, I don't

4    recall those details.

5    Q.   OK.  But you do recall that once they were set up, only

6    Patrick had access to those, right?

7    A.   I don't know if that is an accurate statement.

8    Q.   It's not, or you don't remember?

9    A.   I don't remember.

10   Q.   OK.  Well, you testified on direct that the ESXi server

11   administrator doesn't have, necessarily have access to the VMs,

12   right?

13   A.   That would be my understanding.  That's correct.

14   Q.   OK.  And that's set up because the ESXi administrator, his

15   role, I think, that you testified he's only -- his role is a

16   physical component, correct?

17   A.   For how that translated into virtual environment, that's

18   correct.

19   Q.   OK.  So you can't, with a root server key on an ESXi

20   server, you can't access the virtual machines just with that,

21   right?

22   A.   Not within the virtual machines.  That's my understanding.

23   Q.   OK.  But the role of that ESXi system administrator is,

24   essentially encompasses power-offs, power-ons, snapshots,

25   reversions, right?

M6sWsch5                         Weber - Cross

1    A.   That is my understanding.  That is correct.

2    Q.   OK.  And typically, the standard operations for production

3    servers is that, you know, those servers are supposed to be up

4    as much as possible, right?

5    A.   I can't speak to what the standard is, but that -- that is

6    generally what I would assume.

7    Q.   OK.  You have experience in system administration, right?

8    A.   That is correct.

9    Q.   OK.  And if you were going to take a product offline that

10   people were relying on, you would send out the message to

11   everyone before that, right?

12   A.   I would see that as a best practice, correct.

13   Q.   OK.  And that's for any maintenance or upgrades, right?

14   A.   Generally speaking, I think it is best to warn users of

15   potential outages.

16   Q.   OK.  And you would try to do maintenance or upgrades

17   outside normal working hours, correct?

18   A.   We -- we typically didn't because we were a nine-to-five

19   shop, so --

20          THE COURT:  What do you mean by that?  You typically

21   didn't do outages?

22          THE WITNESS:  So, most -- I can't say most, but in a

23   perfect world, your system administration, when it comes to

24   outages, would be accomplished outside of business hours.

25   Most -- again, I probably shouldn't say most.  But IT shops

1    would probably have a around-the-clock staff to work on that.

2    EDG and ISB, we, we didn't have 24-hour staffing.  It was

3    typically -- everybody had their own hours, but typically, it

4    was a nine to five-type job.  So you couldn't schedule

5    maintenance outside of typical business hours, because

6    everybody's business hours tended to be Monday through Friday

7    from nine to five.

8    BY MR. SCHULTE:

9    Q.  So in any case, even if there was planned maintenance

10   during normal hours, you would still try to notify people,

11   right?

12   A.  That is correct.

13   Q.  OK.  Are you familiar with the Confluence chat feature?

14   A.  Vaguely recall it.  I thought it was -- I thought it was

15   something we looked at implementing but never really did.

16   Q.  OK.  I know it was a long time ago; so you don't recall

17   that feature?

18            MR. LOCKARD:  Objection.

19            THE COURT:  I think he's already answered the

20   question, so sustained.

21   Q.  OK.  Now, there eventually came a point when Patrick left,

22   correct?

23   A.  That is correct.

24   Q.  And you testified on direct that you asked me for

25   assistance, right?

1   A.   That is correct.

2   Q.   And you considered that I was working for you, right?

3   A.   I considered that we were working together.

4   Q.   OK.  But you were aware that Patrick was the one who

5   solicited my assistance, correct?

6          MR. LOCKARD:  Objection to the form.

7          THE COURT:  Overruled.

8   A.   My memory is asking you to be part of it.  I don't know if

9   Patrick asked you as well.

10  Q.   OK.  But Patrick had background in Linux and system

11  administration, right?

12  A.   Patrick had a background in Linux.  I don't know if he had

13  a background in system administration.

14  Q.   OK.  But I had a background in Linux and system

15  administration, correct?

16  A.   If I recall correctly, that is accurate.

17  Q.   OK.  But it's fair to say that there's actually no official

18  record of this transition, right?

19  A.   Not that I am aware of.

20  Q.   There was no branch chief approval, right?

21  A.   Not that I am aware of.

22  Q.   There was no division chief approval, correct?

23  A.   Not that I'm aware of.

24  Q.   There was really no official chain of command or anything,

25  right?

M6sWsch5                          Weber - Cross

1    A.   Again, it was developers taking initiative.

2    Q.   And during this time, at the CIA, through April 2016, you

3    testified that you were a developer, correct?

4    A.   Through April 2016, that's correct.

5    Q.   Well, onto even June of 2016, right?

6    A.   Yes, I still would have been a developer at that time.

7    Q.   You did not work for ISB, right?

8    A.   That is correct.

9    Q.   And you did not set up DevLAN, correct?

10   A.   That is correct.

11   Q.   So you didn't have direct knowledge of DevLAN security or

12   how it was set up, right?

13   A.   That is correct.

14   Q.   OK.  And during this time, you were not a manager, correct?

15   A.   At that time I was not a manager.  That is correct.

16   Q.   And you were not my supervisor, correct?

17   A.   That is correct.

18   Q.   OK.  I just want to kind of go through the levels of

19   permissions on DevLAN to kind of clarify this.  DevLAN is

20   what's called a domain, correct?

21   A.   DevLAN, it -- that is one of the definitions.  It was the

22   DevLAN.net domain.

23   Q.   Just in general, can you explain domains?

24   A.   A domain is a term referring to Active Directory, which is

25   a Microsoft product.  Domain, simply put, is a span of

M6sWsch5                          Weber - Cross

1      influence for computers.  So at the top of a domain you have

2      what's referred to as a domain controller.  Pretty much all

3      security goes through that domain controller.  So

4      authentication of both humans, logging in with username and

5      password, as well as allowing computers to be able to connect

6      to the network would go through the domain.

7      Q.  So administration of the actual DevLAN network is conducted

8      by the domain administrators, correct?

9      A.  The majority of the administration responsibilities, I

10     would assume, fell to them.

11     Q.  And every DevLAN user was also -- let me rephrase it.

12         Every DevLAN user was at least a local administrator for

13     their own workstation, correct?

14     A.  I don't know if that's an accurate statement.

15     Q.  You don't know if every DevLAN user had administrative

16     rights to their own workstation?

17     A.  I don't know if that's true or not.

18     Q.  OK.  And then there were system administrators for the

19     various systems and servers, like the ESXi server, right?

20     A.  I am aware of specifics.  I can't -- I'm talking in

21     generalities if I go beyond what I've already talked to.

22     Q.  OK.  But server and workstation administrators generally

23     invoke their access by logging in to the computers with a

24     password, right?

25     A.  Again, I can't speak to -- I can't speak to the specifics

1    of how it was done across the board.

2    Q.   OK.   I mean is there another way to log in to a computer?

3    A.   There is -- there are numerous ways of being able to log

4    in.   I don't know how every machine on DevLAN was set up.

5    Q.   OK.   But the way you're testifying about the way that we

6    set systems up, on DevLAN there was generally one root account

7    set up on the server, right?

8                MR. LOCKARD:   Objection.   Form.

9                THE COURT:   Sustained.

10   BY MR. SCHULTE:

11   Q.   OK.   On DevLAN, we had one root account with a -- one root

12   account, correct?

13   A.   One root?

14   Q.   OK.   The servers, the virtual machines that were set up

15   were set up with one root account, correct?

16               MR. LOCKARD:   Objection.

17               THE COURT:   Overruled.

18   A.   I believe so.   You were the one that set those up, so I --

19   I don't know.   I don't know if that's an accurate statement for

20   sure.

21               THE COURT:   And just a reminder that root account is

22   an administrator account; is that the same thing?

23               THE WITNESS:   In the Linux world, an admin account is

24   usually referred to as a root account.

25   BY MR. SCHULTE:

1    Q.   But you're aware of the Confluence OSB page, right?

2    A.   Correct.

3    Q.   And on that page was where -- was the aggregation of all

4    server permissions, correct?

5    A.   That is not correct.

6    Q.   For OSB.

7    A.   For shared resources, that was an aggregation of usernames

8    and passwords.

9    Q.   OK.  So generally, the accounts were -- generally, there

10   was one account with a shared password, right?

11   A.    In that scenario, I believe that to be accurate.

12   Q.   OK.  But there was also SSH keys for log-in authentication,

13   right?

14   A.   Again, I know of cases where there was and I know of cases

15   where they weren't.  I can't speak to the in general or the

16   across DevLAN.

17   Q.   Yes.  I'm just specifically talking about the ESXi server

18   and these servers that you have knowledge.

19   A.    I don't know -- I believe the majority -- the majority of

20   the virtual machines that were on, on the ESXi server were

21   Windows machines.  I don't -- I don't think that they would

22   have had SSH keys for logging in.

23   Q.   OK.  So in general, Windows systems, you would use

24   something like remote desktop to log in to those remotely,

25   right?

M6sWsch5                        Weber - Cross

1    A.   That is a way of accessing a Windows machine remotely.

2    Q.   A Windows doesn't generally run an SSH server, correct?

3    A.   Again, I can't speak to how people set up their system.

4    Q.   OK.  Well, let's just move on.  I'm trying to -- OK.

5         The way SSH authentication works is there's a key pair,

6    correct?

7    A.   That's -- that is one way SSH authentication works.

8    Q.   Is there another way to authenticate over SSH?

9    A.   I believe you can use username and password.

10   Q.   OK.  And specifically, about the key pair, can you kind of

11   explain what that means?

12   A.   Sure.  The -- when we're referencing a key pair, we're

13   referencing a public-private encryption.  Asymmetric encryption

14   is the official term.  So the idea, idea behind a key pair is

15   you have your public key and your private key.  Your private

16   key you keep to yourself because that key is what is used to

17   authenticate you, and your public key you share with, with

18   whatever computing resources you want to be able to log in to.

19   So if you -- if somebody loads your public key into their

20   authorized list, it gives you the ability to log in with your

21   private key.

22   Q.   And just to be clear, there's generally just one key pair,

23   correct?

24   A.   Again, generally, there are times where one key pair would

25   be used.  There are times when you would use multiple key

M6sWsch5                         Weber - Cross

1    pairs.  Like, generally is a tough term to answer.

2    Q.  Well, specifically about the servers that you had knowledge

3    during this time in OSB.

4    A.  I -- I can't remember if we used one key pair or multiple

5    key pairs.

6    Q.  OK.  And as you said, the server administrator simply needs

7    to add the user's public key into the authorized key file,

8    right?

9    A.  That is my understanding of Linux, correct.

10   Q.  And that's just like a front key that you can use to open

11   the front door, right?

12             MR. LOCKARD:  Objection.

13             THE COURT:  Sustained.

14   BY MR. SCHULTE:

15   Q.  A user can present his private key and log in to the server

16   without a password, right?

17   A.  If you did not put a password on your private key, that is

18   correct.

19   Q.  And just to clarify that, this would be two different

20   passwords, right?

21   A.  If you -- if you don't use a password reuse, in theory,

22   yes.

23   Q.  No.  I mean there's a password on the key that's different

24   from the password on the server, right?

25   A.  Conceivably, yes.

SOUTHERN DISTRICT REPORTERS, P.C.

(212) 805-0300

1    Q.   OK.   So if you're going to log in to a server and you use

2    your SSH key, you're entering the password to unlock your key,

3    right?

4    A.   If it -- in that scenario, yes.

5    Q.   OK.   And within ESXi specifically, there's a different

6    administration application, correct?

7    A.   That is correct.

8    Q.   OK.   I think it's called vSphere client, right?

9    A.   VSphere client is not the administration application.

10   Q.   OK.   Well, vSphere, right?

11   A.   No.   You're thinking of the tool that you use to interact

12   with the application.

13   Q.   What is the application?

14   A.   VCenter.

15   Q.   VCenter.   So vCenter is installed on the server, right?

16   A.   That is the -- that is one way of doing it.

17   Q.   OK.   But through this administration, it sets up different

18   levels of permissions, correct?

19   A.   You have the ability of applying different levels of

20   permissions through vCenter, correct.

21   Q.   OK.   And the vCenter is going to be completely different

22   permissions than actually logging in to the server, right?

23   A.   I believe that to be correct.   I'm not sure.

24   Q.   OK.   But it has a more fine-grained permission structure,

25   like power users, advanced users, right?

1    A.   Compared to what?

2    Q.   Compared to all or nothing.

3    A.   It does have -- to my knowledge, it does have granular

4    control over what permissions you can grant somebody access to.

5    Q.   And this would be equivalent to the application

6    administration for, like, Stash, right?

7    A.   It's similar.  Obviously different types of permissions.

8    Q.   But the point is this logging in to Stash, logging in to

9    Confluence, there's a difference between the application and

10   the server, right?

11   A.   That is correct.

12   Q.   I think there is confusion because --

13          MR. LOCKARD:  Objection.

14          THE COURT:  Sustained.

15   BY MR. SCHULTE:

16   Q.   OK.  The application name, Stash, is generally installed on

17   a server called Stash, right?

18   A.   In our -- in our deployment, we use the terminology

19   interchangeably.  That is correct.

20   Q.   OK.  And then there's the application itself, access to the

21   web browser, right?

22   A.   Correct.

23   Q.   All right.  Let's move on to development.

24        Project names by themselves are typically unclassified,

25   correct?

1    A.   The intention of the project name is for it to be

2    unclassified.

3    Q.   OK.  Bartender, Margarita, Nader, you cannot tell what

4    these tools do from the name, right?

5    A.   That is the intention of the tool name, is to make it so

6    that you can't -- you can't see what it does.

7    Q.   OK.  I want to touch a little bit about snapshots.  You

8    testified on direct about those, correct?

9    A.   That's correct.

10   Q.   OK.  And it's fair to say that snapshot's are fairly

11   common, correct?

12            MR. LOCKARD:  Objection.

13            THE COURT:  Sustained.

14   BY MR. SCHULTE:

15   Q.   During your work as a developer, on DevLAN, snapshots were

16   fairly common, correct?

17   A.   Generally speaking, for the development and test VMs that

18   we had, usually you would expect to see a snapshot of a known

19   good state.

20   Q.   OK.  So just to walk through how this snapshot reversion

21   works, if you need to perform a reversion to conduct a test,

22   the first step would be to take a snapshot, right?

23   A.   If a snapshot didn't already exist.

24   Q.   OK.  So if the snapshot doesn't already exist, you would

25   take the snapshot, and it's basically a checkpoint, right?

M6sWsch5                        Weber - Cross

1    A.   That's an accurate statement.

2    Q.   OK.   And then after you take this checkpoint, basically,

3    its purpose is to preserve this state so you can return to it,

4    right?

5    A.   That is the intention of it.

6    Q.   OK.   Because if you do a reversion without a snapshot, you

7    just lost your data, right?

8    A.   Correct.

9    Q.   So it's very common -- it's required, really, that you take

10   a snapshot first, correct?

11   A.   Context?   I mean if you would like to be able to have a

12   checkpoint that you could return to, yes, you would need to

13   take a snapshot of that.

14   Q.   OK.   And then after that snapshot is taken, at that point

15   you would execute a reversion to some other snapshot, correct?

16            MR. LOCKARD:   Objection.

17            THE COURT:   Can you rephrase the question,

18   Mr. Schulte?

19            (Defendant conferred with standby counsel)

20   BY MR. SCHULTE:

21   Q.   Once you've established the checkpoint that preserves the

22   system state, then you can freely execute a reversion, correct?

23   A.   If you need to, that is correct.

24   Q.   OK.   And after you execute that reversion, you're in a

25   different system state, correct?

1   A.   Theoretically.  I mean if you made changes to the system

2   and you reverted back to a snapshot, those changes would be

3   discarded.

4   Q.   OK.  But at some point, whenever you're finished, you will

5   need to return back to the checkpoint, correct?

6   A.   No, that's not --

7           MR. LOCKARD:  Objection.

8           THE COURT:  I'll allow it.

9           Go ahead.

10  A.   That's not an accurate statement.

11  Q.   That's not an accurate statement?  Can you explain?

12  A.   You said that I would have to return to snapshot.  I

13  think -- I think the more -- the more likely scenario is a

14  snapshot is meant to be a fallback option that you don't need

15  to fall back to if you don't want to.  I created a lot of

16  snapshots that I never reverted to.

17  Q.   OK.  But if you, if you're taking the initial snapshot to

18  preserve the state, right -- that you testified about?

19          MR. LOCKARD:  Objection.  Hypotheticals.

20          THE COURT:  I think, Mr. Schulte, we're in a land far

21  removed from the facts of this case, so let's bring it back

22  to --

23          MR. SCHULTE:  All right.  Let's go on to documents

24  from the CIA.

25  Q.   Have you ever brought documents into the CIA?

1   A.   Into the CIA?

2   Q.   Yes.

3   A.   Yes.

4   Q.   OK.  What about software?

5   A.   Probably.  I don't remember specifics.

6   Q.   OK.  But in fact, you and I collaborated on a project

7   outside the CIA, correct?

8   A.   That is correct.

9   Q.   That was called the EDG Project Wizard, correct?

10            MR. LOCKARD:  Objection.

11            THE COURT:  Sustained.

12            (Defendant conferred with standby counsel)

13   BY MR. SCHULTE:

14   Q.   You're familiar with what that project was, correct?

15   A.   Correct.

16   Q.   OK.  And we developed the software from our homes, right?

17   A.   A significant portion of the development was done at home.

18   Q.   And then we brought that work into the CIA, correct?

19   A.   That is correct.

20   Q.   In fact, developers sometimes download code or snippets

21   from the internet, right?

22   A.   That is correct.

23   Q.   Sometimes we incorporate that into our software, right?

24   A.   Potentially, correct.

25   Q.   There's no policy that prohibited downloading information

M6sWsch5                          Weber - Cross

1    from the internet and moving it over to DevLAN, correct?

2    A.   There were definite limitations on that.

3    Q.   What was the limitation?

4    A.   It was -- there had to be an official, like, use for it.

5    You -- you couldn't download a movie and have it so you can

6    watch on DevLAN or something like that.  That would be a

7    limitation.

8    Q.   OK.  But this policy was simply left up to the developers'

9    good faith, right?

10   A.   I wouldn't agree with that statement.

11   Q.   There was enforcement of this policy somehow?

12   A.   I can't say yes or no to that.

13   Q.   Why?

14   A.   I -- I'm not aware of anybody breaching the policy.

15   Q.   OK.  But there was no mechanism on DevLAN to do any

16   auditing for if someone was watching a movie all day, right?

17   A.   I can't speak to that.  I don't know.

18   Q.   OK.  But developers sometimes write code from home and take

19   that into the CIA, correct?

20   A.   It has happened in the past.

21   Q.   It's happened in the past?  OK.  So have you ever done

22   that?

23   A.   As you just asked, we worked on the project together.

24   Q.   That's true.  OK.  You were aware that I worked on software

25   and brought it into DevLAN, right?

1              MR. LOCKARD:  Objection.  Form.

2              THE COURT:  Sustained.

3    BY MR. SCHULTE:

4    Q.   There were other instances besides Project Wizard where I

5    worked on and brought software into DevLAN, correct?

6    A.   I am aware of one other scenario where you attempted to

7    bring code from home.

8    Q.   Did the attempt fail?

9    A.   You -- we constantly told you not to use that code in -- in

10   the tools that you were developing.  I am not aware of it ever

11   actually making it into a delivery.

12   Q.   OK.  But besides entire projects, you're aware that -- I

13   mean -- let me rephrase that.

14        Aside from complete projects, there's also instances of

15   code, small code snippets that were brought in, right?

16   A.   I can't recall specifics.

17   Q.   All right.  But there was no policy that you couldn't write

18   code outside at home and take that code into DevLAN, right?

19   A.   There -- I believe there was a policy implemented at some

20   point.  I'm not sure the time frame around it.  I don't recall.

21   Q.   OK.  Let's go back to the Project Wizard example.  I mean,

22   yeah, the code that we worked on before, this code was

23   obviously unclassified, right?

24   A.   That is correct.

25   Q.   So an obvious requirement if you're writing code or

M6sWsch5                        Weber - Cross

1    snippets outside of work is it has to be unclassified, right?

2               MR. LOCKARD:  Objection.  Form and relevance.

3    BY MR. SCHULTE:

4    Q.  OK.  Let's move on.  So after bringing in the code, into

5    DevLAN, it would be considered good security practice to then

6    delete those code snippets from your home, right?

7               MR. LOCKARD:  Objection.

8               THE COURT:  Sustained.

9    BY MR. SCHULTE:

10   Q.  OK.  Whenever you took the project that we worked on into

11   the CIA, did you then delete that code from your home?

12   A.  I did not delete the project that we worked on together

13   from home.  It was more once it made it in, you never took it

14   back out.

15   Q.  OK.  But that code that you developed at your home, you

16   didn't delete that?

17   A.  I don't believe so.  I don't recall, though.

18   Q.  OK.  But it would be considered good security practice to

19   delete that code, right?

20              MR. LOCKARD:  Objection.

21              THE COURT:  Sustained.

22              (Defendant conferred with standby counsel)

23   BY MR. SCHULTE:

24   Q.  OK.  I want to talk a little bit about cover applications.

25       Just in general, malware, some software is easier to

M6sWsch5                         Weber - Cross

1   exploit than others, right?

2   A.  I think that is a fair general statement.

3   Q.  OK.  And there's many different types of malware, correct.

4   A.  That also is correct.

5   Q.  There's trojan horses, right?

6   A.  That is a category of malware.

7   Q.  And there's different techniques, ███████████████████████,

8   correct?

9            MR. LOCKARD:  Objection.  Relevance.

10           THE COURT:  Sustained.

11  BY MR. SCHULTE:

12  Q.  Well, in searching ████████████████████████████████████

13  ████████████████████████, correct?

14           MR. LOCKARD:  Objection.  Relevance.

15           THE COURT:  Sustained.

16  BY MR. SCHULTE:

17  Q.  All right.  Are you familiar with what's called portable

18  apps?

19  A.  I am.

20  Q.  OK.  And you're aware that portable apps are frequent

21  targets for malware, right?

22  A.  I don't know if that's an accurate statement or not.

23  Q.  OK.  But you do -- portable apps are simply portable

24  versions of standard software, right?

25  A.  At the time that portable apps existed and I was aware of

M6sWsch5                         Weber - Cross

1   it, that was what they were.  I don't know if they're still a

2   thing or not.

3   Q.  OK.  But the purpose would be to install a program on a

4   thumb drive that you can then use on a computer you don't own,

5   right?

6   A.  I think that is a purpose -- well, the installation on a

7   thumb drive, I think, is a purpose.

8   Q.  I'm sorry.  I didn't hear that.

9   A.  Sorry.  Installation on a thumb drive, I believe, is a

10  purpose.

11  Q.  OK.  So portable apps ▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋

12  ▋▋▋▋▋▋▋▋▋▋▋, correct?

13          MR. LOCKARD:  Objection.

14          THE COURT:  Sustained.

15  BY MR. SCHULTE:

16  Q.  OK.  Through your experience as a developer, it's common to

17  test ▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋, right?

18          MR. LOCKARD:  Objection.

19          THE COURT:  Do you know what ▋▋▋▋▋▋▋▋▋▋▋▋ is?

20  Can you explain what that term is to you?

21          THE WITNESS:  In the, in the context that he is using

22  it ▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋

23  ▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋▋

24  ▋▋▋▋▋▋▋▋▋▋▋

25          THE COURT:  Can you explain what you mean by that?

M6sWsch5                         Weber - Cross

1            MR. LOCKARD:  Your Honor, I think this may require a

2    conversation.

3            THE COURT:  All right.  Let's move on to a different

4    line, and we'll take it up at the end of the day.

5            Go ahead.

6    BY MR. SCHULTE:

7    Q.   OK.  I want to talk a little bit about TOR.  You're

8    familiar with TOR, right?

9    A.   At a high level.

10   Q.   And TOR was created by the U.S. government, correct?

11   A.   I don't know if that's a correct statement or not.

12   Q.   OK.  All right.  What about Linux distributions; are you

13   familiar with Linux distributions?

14   A.   A very limited understanding of them.

15   Q.   OK.  But you've heard of different flavors of Linux, as

16   it's called, right?

17   A.   That's correct.

18   Q.   And in fact, CentOS was used on -- was installed on the

19   virtual machines, right?

20   A.   I -- from my recollection, I believe that is accurate.

21   Q.   And you're familiar with Debian, correct?

22   A.   Familiar with it, yes.

23   Q.   OK.  And what about Tails?

24   A.   I know what Tails is, but not -- I can't say I'm familiar

25   with it.

1    Q.  It's just another Linux distribution, right?

2              MR. LOCKARD:  Objection.

3              THE COURT:  Sustained.

4    BY MR. SCHULTE:

5    Q.  You understand that Tails is a Linux distribution, correct?

6              MR. LOCKARD:  Objection.

7              THE COURT:  Sustained.

8              (Defendant conferred with standby counsel)

9    BY MR. SCHULTE:

10   Q.  You used CentOS before, correct?

11   A.  Yes.

12   Q.  OK.  And other Linux distributions, right?

13   A.  Yes, that's correct.

14   Q.  And you said that you have knowledge about Tails, correct?

15   A.  I just have heard it, and I generally attribute it to usage

16   of TOR.  But that's -- that's the extent of my knowledge of

17   Tails.

18   Q.  OK.  But you know what Tails is, right?

19             MR. LOCKARD:  Objection.

20             THE COURT:  Sustained.

21             Let's move on, please.

22   BY MR. SCHULTE:

23   Q.  OK.  Do you know what hashing is?

24   A.  I do.

25   Q.  Developers at the CIA employ hashing all the time, correct?

M6sWsch5                          Weber - Cross

1          MR. LOCKARD:  Objection.

2          THE COURT:  Sustained.

3   BY MR. SCHULTE:

4   Q.  Developers in general employ hashing all the time, correct?

5   A.  Again, in general, I can't speak to what the generality --

6   what general uses were.

7   Q.  Well, you and I have developed software that uses hashing,

8   right?

9          MR. LOCKARD:  Objection.

10          THE COURT:  Overruled.

11  A.  That's correct.

12          THE COURT:  Actually, can you break that up and do it

13  as two questions.  First, have you developed software that has

14  used hashing?

15          THE WITNESS:  That is a correct statement.

16          THE COURT:  And to your knowledge, did Mr. Schulte,

17  when he worked at the CIA, develop software that used hashing?

18          THE WITNESS:  That is a correct statement.

19          THE COURT:  OK.

20  BY MR. SCHULTE:

21  Q.  And MD5 is just one of many hashing algorithms, correct?

22  A.  That is correct.

23  Q.  And as a developer, I know how to calculate an MD5, right?

24          MR. LOCKARD:  Objection.

25          THE COURT:  Sustained.

M6sWsch5                        Weber - Cross

1    BY MR. SCHULTE:

2    Q.  As a developer, you know how to calculate an MD5, right?

3    A.  I don't think I know the math behind how to calculate an

4    MD5.  I've implemented it.

5    Q.  OK.  Well, you've calculated an MD5 before, right?

6    A.  I have leveraged libraries to calculate an MD5.

7    Q.  There's software that exists that will calculate an MD5 for

8    you, right?

9    A.  That is correct.

10   Q.  And then you don't have to do any math, right?

11   A.  That is correct.

12   Q.  OK.  I want to pull up Government Exhibit 1704.  OK.  Slide

13   53.  Do you recognize these types of Google searches?

14          MR. LOCKARD:  Objection.  Foundation.  Relevance.

15          THE COURT:  I'll sustain to that particular question.

16          But next question, Mr. Schulte.

17   BY MR. SCHULTE:

18   Q.  OK.  In software development, it's common to use Google to

19   do research, correct?

20   A.  I think that's a safe statement.

21   Q.  OK.  And in doing research, you would search Google for

22   algorithms, correct?

23          MR. LOCKARD:  Objection.  Hypothetical.

24          THE COURT:  Overruled.

25   A.  That is a, something that you could look up via Google.

1    Q.  OK.  But implementing, when you actually are writing

2    software to implement hashing algorithms, you have to have some

3    kind of reference to do that, right?

4    A.  Not necessarily.

5    Q.  OK.  It's common to have reference material to write the

6    code, right?

7    A.  It's not unheard of.

8    Q.  OK.  If you don't know how to implement a hashing

9    algorithm, you would search for it, correct?

10             MR. LOCKARD:  Objection.

11             THE COURT:  Overruled.

12   A.  That is -- that is a way you could approach the problem.

13   That is correct.

14   Q.  OK.  And these searches and Google searches on the page

15   here would represent that type of research, correct?

16             MR. LOCKARD:  Objection.

17             THE COURT:  Sustained.

18             (Defendant conferred with standby counsel)

19   BY MR. SCHULTE:

20   Q.  You're familiar with C++, correct?

21   A.  That's correct.

22   Q.  That's a programming language, right?

23   A.  That's correct.

24   Q.  And if you, if you're researching programming-related

25   questions, you would include that on your search, right?

M6sWsch5                         Weber - Cross

1           MR. LOCKARD:  Objection.

2           THE COURT:  Sustained.  Can I see the parties at

3    sidebar, please.

4           (Continued on next page)

1          (At sidebar)

2          THE COURT:  Putting aside relevance questions, it

3     seems to me that you're improperly trying to use this witness

4     as an expert witness.  Putting aside whether he's even

5     competent to be an expert witness on some of the subjects

6     you're inquiring about, you didn't notice him as an expert

7     witness.  So I think a lot of this is just improper testimony,

8     whether it is treated as your expert or not.

9          MR. SCHULTE:  Well, whenever I was crossing the

10    experts, they said they didn't have knowledge of DevLAN or what

11    would be worked on, so a lot of that cross I couldn't do.  So

12    that's what, he has the knowledge of DevLAN, software.  It's

13    not an expert opinion; it's just his work.  Right?

14         THE COURT:  You're literally asking him for his

15    opinion on whether somebody doing that search would be engaged

16    in essentially writing software for part of your job.  That's

17    an expert opinion.

18         MR. SCHULTE:  That's an expert opinion, to say what

19    his -- I'm not saying, I'm not trying to get his expert opinion

20    but just from his background.

21         THE COURT:  From his training expertise.  That's the

22    point.  In other words, this is not something within his lay

23    experience or something that would be within the ken of an

24    average juror or person.  This is something that requires

25    expertise, and you're attempting to elicit or leverage his

M6sWsch5                        Weber - Cross

1    expertise and you didn't notice him as an expert.

2              MR. SCHULTE:  I mean the CIA witnesses wouldn't talk

3    to any of us.  There was no way to notice him, right?

4              THE COURT:  No.  I mean --

5              MR. SCHULTE:  I don't have any statements from him or

6    testimony as to what he would testify to, so I don't know what

7    his testimony would be.

8              THE COURT:  But if you intended to elicit expert

9    testimony from him, you had to notice him as an expert.  If he

10   wouldn't talk to you, you needed to find another expert.

11             (Defendant conferred with standby counsel)

12             MR. SCHULTE:  He's just testifying to what an average

13   developer in EDG would know, not necessarily --

14             THE COURT:  No.  You're asking him about tools that

15   he's never used.  You've asked him about searches that he

16   hasn't personally conducted.  You're not.  I understand that it

17   comes close to what he did for his job and in that sense it's

18   close to fact testimony, which is why it hasn't all been

19   improper, but a lot of it is, I think, demonstrably improper.

20             Anything, Mr. Lockard, you want to say?

21             MR. LOCKARD:  Yes, your Honor.

22             I think this line of questioning implicates also the

23   January 30, 2020, CIPA order, which laid out some parameters

24   about what is proper to elicit on cross-examination about tool

25   development and about operations.  It seems that Mr. Schulte is

M6sWsch5                         Weber - Cross

1    clearly trying to elicit testimony to suggest that he used

2    particular tools and techniques for work, and that's why he was

3    conducting these Google searches, and I think that steps

4    outside the bounds of the CIPA order.  And Mr. Schulte, despite

5    extensive CIPA litigation, relitigation in advance of this

6    trial, did not give notice of those particular areas of

7    testimony.

8             THE COURT:  I think that the CIPA order, the portion

9    that I read, said that he was allowed to cross-examine

10   witnesses to establish that Google searches would have been

11   things that he would have done within the ordinary course of

12   his work.  So I think it's consistent with the CIPA order.  But

13   my concern is a separate one, that he is trying to use this

14   witness to elicit expert testimony.

15            MR. LOCKARD:  And I think there's a prior cross that

16   did not involve Google searches that Mr. Schulte tried to delve

17   into.

18            THE COURT:  I agree that there's some, and maybe we'll

19   talk about the particulars later, but I think some of it is

20   probably intended to lay a foundation to make an argument about

21   the Google searches which I think would be potentially proper.

22            MR. LOCKARD:  Yes.

23            THE COURT:  Mr. Schulte, anything else?

24            (Defendant conferred with standby counsel)

25            MR. SCHULTE:  Yeah, so I think the biggest issue here

M6sWsch5                    Weber - Cross

1       is because of the kind of teetering around the classified

2       information, you have to do it in generalities or situations or

3       circumstances.  So if I can't testify -- so, for example, the

4       portable app-type stuff, if I can't say specifically some

5       portable app was tied to something else or these searches, you

6       know, then I have to say in general, is this how the developers

7       would do something, or is this how something would work.

8               That's why that kind of testimony, whereas normally,

9       you know, it would be too generic and you have to be specific,

10      I can't get specific.  So that's why I think that kind of

11      testimony should be permissible here.

12              THE COURT:  I think if you had a particular CIA tool

13      that you worked on that you believed either you were going to

14      testify or cross-examine someone to establish that this Google

15      search was connected to a particular tool, it was incumbent

16      upon you to identify that in the CIPA process, which is not to

17      say that you can't go into some of this in general terms.  But

18      I don't think you can use this witness as an expert.

19              We have about six minutes remaining on the trial day,

20      so let's finish it up.  But I would limit yourself to fact

21      testimony from this witness, not expert testimony.

22              We'll discuss the parameters beyond that after 2:45.

23      OK?

24              (Continued on next page)

25

M6sWsch5                          Weber - Cross

1           (In open court)

2           THE COURT:  All right.  Thank you for your patience,

3    ladies and gentlemen.

4           Mr. Schulte, you may continue.

5    BY MR. SCHULTE:

6    Q.  All right.  I want to talk a little bit about your

7    testimony on direct about the mount command.  Do you remember

8    that?

9    A.  Yes, I do.

10   Q.  OK.  So you testified on direct about using this mount

11   command in your VM, correct?

12   A.  That's correct.

13   Q.  And this mount command is necessary in order to access the

14   Altabackups, correct?

15   A.  I believe that to be accurate.

16   Q.  OK.  And can you -- well, your VM is located on your

17   computer, right?

18   A.  That's correct.

19   Q.  OK.  And you also testified about me showing you on my

20   computer, right?

21   A.  I believe my testimony was you showing me how to do the

22   mount command.

23   Q.  OK.  And that was on my computer, correct?

24   A.  I -- my recollection is you telling me what to do as I

25   typed it on my machine.

1    Q.   OK.  So your recollection is we were in your cube, and I

2    was just driving you through the mount?

3    A.   That's what I remember.

4    Q.   OK.  And I'm going to pull up what's in evidence as defense

5    exhibit 1201.  And you're familiar with what this shows,

6    correct?

7    A.   I don't know what this shows.

8    Q.   OK.  So you don't know what this is?

9    A.   I would be guessing.

10              THE COURT:  All right.  Let's take it down.

11              Next.

12   BY MR. SCHULTE:

13   Q.   So DevLAN contained all kinds of different hardware,

14   correct?

15   A.   It contained different hardware.  That is correct.

16   Q.   Different kinds of software, right?

17   A.   That is also correct.

18   Q.   Computers could be connected to DevLAN, right?

19   A.   That is the point of a network.  That is correct.

20   Q.   Other devices could be connected to DevLAN, right?

21   A.   That is correct.

22   Q.   Hard drives could be obtained from ISB, correct?

23   A.   Correct.

24   Q.   And connected to DevLAN, right?

25   A.   Correct.

M6sWsch5                           Weber - Cross

1    Q.  The same to for thumb drives, right?

2    A.  Correct.

3    Q.  And you used thumb drives, right?

4    A.  That is correct.

5    Q.  Cell phones were connected to DevLAN, correct?

6            MR. LOCKARD:  Objection.

7            THE COURT:  Overruled.

8    A.  I -- I don't know of specific scenarios where cell phones

9    were connected to DevLAN.

10   Q.  OK.  Laptops were connected to DevLAN, correct?

11   A.  Correct.

12   Q.  And wireless laptops were connected, correct?

13   A.  That is correct.

14   Q.  OK.  So do you know how many different types of devices

15   were connected on DevLAN?

16   A.  No, I don't.

17   Q.  And developers had access to the internet in their secure

18   CIA vaults, correct?

19   A.  That is correct.

20   Q.  There were two unclassified networks, right?

21   A.  That is correct.

22   Q.  FIN and ██████, right?

23   A.  That is correct.

24   Q.  And each developer had at least one of these

25   internet-enabled computers next to their DevLAN workstation,

M6sWsch5

1   right?

2   A.   I don't know if that's an accurate statement.

3   Q.   You don't know if everyone had access to the internet?

4   A.   I don't know if everyone had access to the internet.

5   Q.   OK.   But developers could freely connect any number of

6   these devices or removable media into the DevLAN system,

7   correct?

8   A.   I don't know if that's an accurate statement.

9   Q.   OK.   You could get thumb drives and hard drives, right?

10  A.   That is correct.

11  Q.   And you can connect them to DevLAN, right?

12  A.   That is correct.

13  Q.   OK.   Then you could connect it directly to the internet

14  system, right?

15  A.   That would be a significant security violation.

16  Q.   OK.   But technically, it could be done, right?

17  A.   I -- I would guess yes, but I don't know -- I don't know

18  the security posture of the internet-connected networks.

19          THE COURT:   All right.   We're going to call it quits

20  there.   Thank you.

21          Ladies and gentlemen, let me share a couple things

22  with you.

23          First of all, to make things a little easier, we've

24  arranged to provide you with Covid tests to take home with you

25  so that you can take them in the morning before you leave.   You

M6sWsch5

1    don't need to show up early here or report to the District

2    Executive's office.  You can take them in the comfort of your

3    own home.  So as you leave today, Ms. Smallman will give you

4    each a box.  I think that the boxes contain two tests, but in

5    any event, they certainly contain one.  That's No. 1.

6           Second, I told you I'd give you an update on the

7    schedule.  As I told you during voir dire at the beginning of

8    the case, it's always a little hard to know in this business;

9    it's more art than science because things happen, and in a

10   world with Covid, even new things happen.  But the bottom line

11   is I'm pleased to say that we're, I think, generally on

12   schedule, which is to say that I don't think that the case -- I

13   think the case, let me put it this way.

14          I think the case will be done within the time frame

15   that I had told you at the outset.  I had said up to five or

16   six weeks or five weeks as a general time frame, and I think

17   we're certainly on track to do that.  It may even end sooner

18   than that, but I don't think it will go beyond that.

19          I know one of you has travel family plans at the end

20   of next month.  I do not anticipate that this case will pose

21   any issues for that, so hopefully that puts you at ease.

22   Relatedly, I know one of you has travel plans that you were not

23   able to change that involves returning next Tuesday on July 5.

24   After agonizing a bit about it, I've decided that we're going

25   to take that day off.  Given that we've lost one juror already,

M6sWsch5

1    we wouldn't be able to proceed if it was the juror who wouldn't

2    be here on Tuesday, obviously would have to be excused.  I'm

3    just a little worried about losing people along the way.  So

4    rather than that, we're going to take Tuesday off.

5              That does mean a longer break.  That is, we're already

6    off on Friday, as you know, and I'll extend the weekend through

7    Tuesday.  I don't love that, but my sense is that that's the

8    better option than losing another juror, and I promise that I

9    will try to keep things moving to make up for it.

10             Consistent with that, what I'd like you to do -- I'm

11   giving you a little bit of a heads-up so hopefully you can

12   arrange things.  If this causes a problem, let Ms. Smallman

13   know, and I will take it under advisement.  But I would like to

14   potentially sit a longer day next Wednesday and Thursday, just

15   to make up some of the time that we're going to lose on

16   Tuesday.  So if you could plan to be here until, let's say,

17   four or even 4:30 on those days and adjust things accordingly,

18   then we'll make up for some of the lost time.  Because

19   ultimately my goal is to get you guys out of here and returned

20   to your regular civilian lives as quickly as I can.

21             So that's an update on the schedule.  I think

22   generally good news, but my predictions are so far -- no reason

23   to believe that they will be wrong, let's put it that way, so

24   an adjustment to the schedule.

25             With that, my usual instructions apply.  Don't discuss

M6sWsch5

1    the case.  Continue to keep an open mind.  Don't do any

2    research about the case.  And please be here by 8:45 tomorrow.

3    Remember to take your Covid test before you come in.

4              I wish you a very pleasant afternoon and evening.

5    We'll see you form morning.

6              Thank you.

7              (Continued on next page)

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

M6sWsch5

1          THE COURT:  You may be seated.

2          All right.  Mr. Weber, you may step down in a moment.

3   Just a reminder that since you're still on cross, you shouldn't

4   discuss the substance of your testimony with anyone from the

5   government.  Please be in the witness room -- or wherever

6   you're supposed to be, that is -- by 9:00 tomorrow, by a few

7   minutes before 9:00, so that we can start promptly.

8          You may step down.

9          THE WITNESS:  Yes, your Honor.

10          THE COURT:  And I trust that the restrictions in place

11   will be lifted as soon as Mr. Weber is wherever he needs to be

12   so that the courtroom is returned to its fully public status.

13          (Witness not present)

14          THE COURT:  All right.  The witness has left.

15          First, just to circle back to something we discussed

16   earlier, during cross, Mr. Weber testified that he wasn't even

17   aware whether Hickok was part of the WikiLeaks leak, so that is

18   a further point reinforcing my ruling that asking him about

19   whether Hickok was taken offline and the like and standard

20   operating procedures, whatever they may have been, was not a

21   proper line of questioning.  Since to his knowledge, he didn't

22   even know if it was part of the leak, he wouldn't even be in a

23   position to describe the standard operating procedures with

24   respect to or as applied to Hickok.

25          Anything that we need to discuss?

M6sWsch5

1          Again, just to reinforce the point that I said at

2     sidebar, I think a lot of this questioning is trying to use

3     Mr. Weber as an expert witness, and putting aside whether he's

4     even qualified to opine on some of the things that he's being

5     asked about, he wasn't noticed by the defense or by the

6     prosecution, for that matter, as an expert.  So I think it's

7     improper, and I'm going to start cutting you off if you

8     continue to go down that path.

9          Mr. Schulte.

10          MR. SCHULTE:  Yeah.  I was just going to say that in

11    lieu of calling other witnesses about the DevLAN security and

12    stuff, I was trying to go through some of his testimony, for

13    example, from the direct from last trial.  But I think that's

14    coming to the end, so I don't expect that there's going to be

15    much more, and the rest of it will be probably specifically

16    related to his direct.

17          THE COURT:  OK.  And how much more cross do you

18    anticipate there being?

19          MR. SCHULTE:  Right now, there's ten, ten pages, but I

20    intend to go through and, you know, make sure it's just

21    about -- review it before tomorrow to make sure, you know, we

22    can go quicker through it.

23          THE COURT:  OK.  I would urge you to do that.  Ten of

24    how many?  How many have we gone through?

25          MR. SCHULTE:  Ten of 50.

M6sWsch5

1              THE COURT:  The cross has exceeded the direct already.

2              MR. SCHULTE:  Page 10 -- ten pages left out of 50, so

3    about, less than 20 percent left.

4              THE COURT:  All right.  Good to know.

5              All right.  Anything to discuss from the government?

6    I don't know if you want to speak to the transcript, which you

7    started discussing earlier, if we can circle back to any of the

8    issues that were left open this morning.

9              MR. LOCKARD:  Our update from lunch may be out of

10   date, but at least as of lunch, we had received the transcript

11   shortly before the morning session began, and after being

12   reviewed, we expect there will be some redactions that will be

13   proposed.  But we'll circle up after we conclude here and

14   report back.

15             THE COURT:  OK.  And this is with respect to

16   yesterday's transcript?

17             MR. LOCKARD:  That's right.

18             THE COURT:  OK.  Try and do that as expeditiously as

19   you can so that Mr. Schulte can have it with him in the MDC.

20             And 820-224 or the IRC chats, any updates there, or

21   should we table that?

22             MR. LOCKARD:  We're still not within spitting distance

23   of those becoming live issues, but we will have them resolved

24   by the time they do.

25             THE COURT:  All right.  And did you want to circle

M6sWsch5

1     back on the last issue I had raised as to AFD and the Link

2     chat?

3              MR. DENTON:  Sure, your Honor.

4              First of all, I think as to the substance of the point

5     about whether there's *Brady* there, I don't think there is

6     anything inconsistent with what Mr. Leedom testified to there.

7              The observation is that backups to the Atlassian

8     products were on the file share, the NetApp, which every DevLAN

9     user had access to.  Those are undisputed points.  The question

10    of whether that particular folder was controlled in some way or

11    what they were, you know, that's a separate question.  That's

12    not addressed by Special Agent Evanchec's message.

13             Mr. Schulte tried very hard to get Special Agent

14    Evanchec to answer any number of questions about Link messages

15    but chose not to ask him about this one.  So he's sort of

16    foregone the opportunity to have him clarify it.  And we've

17    provided the 302 that sort of lays out what AFD was looking at,

18    and there, too, I don't think there's anything inconsistent.

19             I will say even to the extent that the defendant

20    believed it was helpful because it was *Brady*, that's a separate

21    question from his obligation to give Section 5 notice.  He

22    still would have to give notice and would have to go through

23    the process of what form was necessary for him to vindicate

24    that right.  But we're not even there, because I don't think it

25    bears the weight he gives it, and he decided not to ask about

1      it with the witness on the stand.

2               MR. SCHULTE:  To the degree that we have to go through

3      Section 5, Section 5 is only to declassify information that I

4      know.  I obviously have no idea what this information would

5      reveal from AFD because I've never been provided it.  So we

6      could never have gone through CIPA 5 and there was nothing for

7      me to notice because I have no idea what AFD reports said or

8      didn't say.

9               I think to the degree that the government still

10     maintains that AFD, there's no reports or AFD didn't conduct

11     any technical review, the simple two questions for the witness

12     is if there are reports and AFD determined that there were

13     public access to the servers.  That's huge for the defense.

14     And I think based on the Link messages and the 302, that

15     there's, the defense has a good faith belief that this is true

16     or that there is other examinations conducted by AFD that would

17     show something favorable to the defense.

18               THE COURT:  All right.

19               This pertains to Mr. Schulte's desire to call a

20     particular witness, and the government has moved to quash the

21     subpoena and preclude that witness and I'll grant that motion.

22     I had indicated that there were two scenarios in which I might

23     conclude otherwise:  First, if I was persuaded that the subject

24     matter of the proposed testimony was not classified and gave

25     Mr. Schulte an opportunity to persuade me that that was the

1    case, and I'm not persuaded for the reasons I discussed earlier

2    today.

3             Second was in the event that there was any potential

4    *Brady* violation, then I would consider Mr. Schulte's failure to

5    comply with CIPA, essentially consider whether it should be

6    overlooked as a remedy for a *Brady* violation.  But I'm

7    persuaded that there is no *Brady* violation and that the

8    witness, in any event, would not be in a position to even

9    testify about the things that are referenced in that Link

10   message.  Nor do I think that the Link message is inconsistent

11   with anything that the government has presented in this case.

12            So given that Mr. Schulte has not carried his burden

13   on either of the two issues I gave him an opportunity to

14   demonstrate, the government's application is granted as to that

15   witness.

16            All right.  Anything else that we need to discuss here

17   and now?  I have another matter in 15 minutes or so, so let me

18   get to it.

19            MR. DENTON:  Just very quickly.

20            Tomorrow, your Honor, the witness coming after this

21   will also be someone in the closed session.  I sincerely hope

22   that we can both finish Mr. Weber and finish that witness, who

23   I expect to be very short, and start with a third tomorrow.

24   Hope springs eternal.  If we get that far, that third witness

25   would be in the open courtroom, so we would just need to -- I

M6sWsch5

1    think that change can be made more unobtrusively.  We just need

2    to have the CSOs to let anyone walk in, but just flagging that

3    we'll have to make the shift at that point.

4             THE COURT:  All right.

5             Any idea how quickly that change can be made; that is

6    to say, how long it takes the witness to clear whatever area

7    the witness needs to clear before the restrictions are lifted?

8    I think the lifting can be done almost instantaneously; it's

9    more of the witness getting wherever the witness needs to go.

10            MR. DENTON:  I think quite quickly, your Honor, so,

11   you know, no more than a couple of minutes.  And to the extent

12   that you wanted to excuse the jury to the jury room only rather

13   than to downstairs, that would be more than enough time.

14            THE COURT:  OK.  I'll take that under advisement.

15   Perhaps what the government should do is -- well, I assume that

16   the next witness wouldn't even be here until the restrictions

17   are lifted, right?

18            MR. DENTON:  Not in the courtroom, but we'd be able to

19   have the next witness on the floor, nearby.

20            THE COURT:  OK.  Maybe what we should do at a minimum

21   is I'll allow you to call the next witness, and then you can

22   take a minute or two to get the witness while the other witness

23   clears the floor, or whatever the case may be.  And then once

24   that witness comes in, I'll assume that the restrictions have

25   been lifted, and we're back to a fully public courtroom.

M6sWsch5

1          Does that make sense?

2              MR. DENTON:  Yes, your Honor.

3              THE COURT:  If it makes it easier to excuse the jury,

4    I may do that.  It also depends on where we are in the day and

5    whether I think that's appropriate.

6              MR. DENTON:  I think we can do that quickly enough

7    that we could accomplish it during a stand up and stretch, your

8    Honor.

9              THE COURT:  All right.

10             We'll finish with Mr. Weber.  And then it's

11   Mr. Stedman, is that correct?

12             MR. DENTON:  That's correct, your Honor.

13             THE COURT:  And who is after that?

14             MR. DENTON:  Sean Roche.

15             THE COURT:  And do you think we would get beyond

16   Mr. Roche?

17             MR. DENTON:  I doubt it.  I think the direct for each

18   of Mr. Stedman and Mr. Roche is somewhere in the 45 minutes to

19   an hour range.  So with cross-examination, I think finishing

20   Mr. Weber plus the two of them will easily get us to the end of

21   the day.

22             THE COURT:  All right.  And I know you have a witness

23   coming up who I understand requires an interpreter.  Is that

24   correct?

25             MR. DENTON:  Yes, your Honor.  That will be, I guess,

M6sWsch5

1    the fourth witness, Carlos Betances, after Mr. Roche.

2            THE COURT:  OK.  I just wanted to have a sense of the

3    timing.

4            Any other issues that we should discuss now?

5            MR. DENTON:  Not from us, your Honor.

6            THE COURT:  Mr. Schulte, anything else?

7            MR. SCHULTE:  I think there's just an issue that we

8    were informed that it would be Betances before Roche, so we

9    prepared that way.

10           THE COURT:  OK.  Well, now you know that it may go the

11   other way, so I trust that you will prepare whatever you need

12   to prepare.

13           Anything else?

14           MR. SCHULTE:  No.

15           THE COURT:  Hang on one second.

16           All right.  Just to flag something.  I'm not, I think,

17   asking for anyone's views just yet, but juror No. 13, you may

18   recall, has some sort of leg or knee issue, and he had told me

19   during voir dire that he just couldn't sit, that either

20   standing or putting his leg up was required, and as you'll

21   recall, he's sitting in a spot where he can do that.

22   Nevertheless, he has told my deputy that he is quote/unquote in

23   too much pain.  I don't entirely know what that means.

24   Obviously, I want to make sure that he's able to focus on the

25   testimony and evidence, and it may make sense to inquire to

M6sWsch5

1    find out.  But why don't you give it some thought, and we can

2    discuss in the morning how to handle that.  In the meantime --

3    well, why don't we leave it there.

4              All right.  Anything else before I go?

5              MR. LOCKARD:  No, Judge.

6              THE COURT:  Mr. Schulte.

7              MR. SCHULTE:  No.  Nothing further.

8              THE COURT:  All right.  In that case, I will see you

9    tomorrow morning.

10              Thank you very much.

11              We are adjourned for the day.

12              (Adjourned to June 29, 2022, at 9:00 a.m.)

13

14

15

16

17

18

19

20

21

22

23

24

25

14

15

16

17

18

19

20

21

22

23

24

25